

#	Audit Type	Section	Key Activity
1	Privacy	§164.502(a)(5)(i)	Prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes
2	Privacy	§164.502(f)	Deceased individuals

3

Privacy

§164.502(g)

Personal
representatives

4

Privacy

§164.502(h)

Confidential
communications

5	Privacy	§164.502(i)	Uses and disclosures consistent with notice
6	Privacy	§164.502(j)(1)	Disclosures by whistleblowers
7	Privacy	§164.502(j)(2)	Disclosures by workforce members who are victims of a crime

8

Privacy

§164.504(e)

Business associate
contracts

9	Privacy	§164.504(f)	Requirements for group health plans
11	Privacy	§164.506(a)	Permitted uses and disclosures
12	Privacy	§164.506(b); (b)(1); and (b)(2)	Consent for uses and disclosures

13

Privacy

§164.508(a)(1-3) and
§164.508(b)(1-2)

Authorizations for uses
and disclosures is
required

14

Privacy

§164.508(b)(3)

Compound
authorizations --
Exceptions

15

Privacy

§164.508(b)(4)

Prohibition on conditioning of authorizations

16

Privacy

§164.508(b)(6) and §164.508(c)(1-4)

Uses and Disclosures for which an Authorization is Required – Documentation and Content

17	Privacy	§164.510(a)(1) and §164.510(a)(2)	Use and Disclosure for Facility Directories; Opportunity to Object
18	Privacy	§164.510(a)(3)	Uses and Disclosures for Facility Directories in Emergency Circumstances
19	Privacy	§164.510(b)(1)	Permitted uses and disclosures
20	Privacy	§164.510(b)(2)	Uses and disclosures with the individual present
21	Privacy	§164.510(b)(3)	Limited uses and disclosures when the individual is not present

22	Privacy	§164.510(b)(4)	Uses and disclosures for disaster relief purposes
23	Privacy	§164.510(b)(5)	Uses and disclosures when the individual is deceased
24	Privacy	§164.512(a)	Uses and disclosures required by law

25

Privacy

§164.512(b)

Uses and disclosures
for public health
activities

26

Privacy

§164.512(c)

Disclosures about
victims of abuse,
neglect or domestic
violence

27

Privacy

§164.512(d)

Uses and disclosures
for health oversight
activities

28

Privacy

§164.512(e)

Disclosures for judicial
and administrative
proceedings

29

Privacy

§164.512(f)(1)

Disclosures for law
enforcement purposes

30	Privacy	§164.512(f)(2)	Disclosures for law enforcement purposes - for identification and location -
31	Privacy	§164.512(f)(3)	Disclosures for law enforcement purposes-- PHI of a possible victim of a crime
32	Privacy	§164.512(f)(4)	Disclosures for law enforcement purposes-- an individual who has died as a result of suspected criminal conduct
33	Privacy	§164.512(f)(5)	Disclosures for law enforcement purposes: crime on premises

34	Privacy	§164.512(f)(6)	Disclosures for law enforcement purposes
35	Privacy	§164.512(g)	Uses and disclosures about decedents
36	Privacy	§164.512(h)	Uses and disclosures for cadaveric organ, eye or tissue donation

37

Privacy

§164.512(i)(1)

Uses and disclosures
for research purposes --
Permitted Uses and
Disclosures

38

Privacy

§164.512(i)(2)

Uses and disclosures
for research purposes --
Documentation of
Waiver Approval

39

Privacy

§164.512(k)(1)

Uses and disclosures
for specialized
government functions --
Military

40	Privacy	§164.512(k)(2)	Uses and disclosures for specialized government functions -- National Security and intelligence activities
41	Privacy	§164.512(k)(3)	Uses and disclosures for specialized government functions -- Protective Services
42	Privacy	§164.512(k)(4)	Uses and disclosures for specialized government functions -- Medical Suitability Determinations
43	Privacy	§164.512(k)(5)	Uses and disclosures for specialized government functions -- Correctional institutions
44	Privacy	§164.512(k)(6)	Uses and disclosures for specialized government functions -- Providing public benefits

45	Privacy	§164.512(l)	Disclosures for workers' compensation
----	---------	-------------	---------------------------------------

46	Privacy	§164.514(b) & §164.514(c)	Requirements for De-Identification of PHI & Re-Identification of PHI
----	---------	---------------------------	--

47	Privacy	§164.514(d)(1)- §164.514(d)(2)	Standard: Minimum Necessary & Minimum Necessary Uses of PHI
48	Privacy	§164.514(d)(3)	Minimum Necessary - Disclosures of PHI
49	Privacy	§164.514(d)(4)	Minimum Necessary requests for protected health information

50

Privacy

§164.514(d)(5)

Minimum Necessary -
Other content
requirement

51

Privacy

§164.514(e)

Limited Data Sets and
Data Use Agreements

52

Privacy

§164.514(f)

Uses and Disclosures
for Fundraising

53

Privacy

§164.514(g)

Uses and Disclosures
for Underwriting and
Related Purposes

54

Privacy

§164.514(h)

Verification
Requirements

55

Privacy

§164.520(a)(1) & (b)(1)

Notice of Privacy
Practices

56

Privacy

§164.520(c)(1)

Provisions of Notice -
Health Plans

57

Privacy

§164.520(c)(2)

Provisions of Notice -
Certain Covered Health
Care Providers

58

Privacy

§164.520(c)(3)

Provision of Notice -
Electronic Notice

59

Privacy

§164.520(d)

Joint Notice by
Separate Covered
Entities

60	Privacy	§164.520(e)	Documentation
----	---------	-------------	---------------

61	Privacy	§164.522(a)(1)	Right of an Individual to Request Restriction of Uses and Disclosures
----	---------	----------------	---

62	Privacy	§164.522(a)(2)	Terminating a Restriction
----	---------	----------------	---------------------------

63	Privacy	§164.522(a)(3)	Documentation
----	---------	----------------	---------------

64	Privacy	§164.522(b)(1)	Confidential Communications Requirements
----	---------	----------------	--

65	Privacy	§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)	Right to access
----	---------	--	-----------------

66	Privacy	§164.524(d) (2)	Denial of Access
----	---------	-----------------	------------------

67	Privacy	§164.524(a)(2)	Unreviewable grounds for denial
----	---------	----------------	---------------------------------

68	Privacy	§164.524(a)(3)	Reviewable grounds for denial
----	---------	----------------	-------------------------------

69	Privacy	§164.524(a)(4) & (d)(4)	Review of denial of access
----	---------	-------------------------	----------------------------

70	Privacy	§164.524(e)	Documentation
----	---------	-------------	---------------

71

Privacy

§164.526(a)(1)

Right to Amend

72

Privacy

§164.526(a)(2)

Denying the
Amendment

73

Privacy

§164.526(c)

Accepting the
Amendment

74

Privacy

§164.526(d)

Denying the
Amendment

75

Privacy

§164.528(a)

Right to an Accounting
of Disclosures of PHI

76

Privacy

§164.528(b)

Content of the
Accounting

77

Privacy

§164.528(c)

Provision of the
Accounting

78

Privacy

§164.528(d)

Documentation

79	Privacy	§164.530(a)	Personnel designations
80	Privacy	§164.530(b)	Training
81	Privacy	§164.530(c)	Safeguards
82	Privacy	§164.530(d)(1)	Complaints to the Covered Entity
83	Privacy	§164.530(d)(2)	Complaints to the Covered Entity

84	Privacy	§164.530(e)(1)	Sanctions
----	---------	----------------	-----------

85	Privacy	§164.530(f)	Mitigation
----	---------	-------------	------------

86	Privacy	§164.530(g)	Refraining from Intimidating or Retaliatory Acts
----	---------	-------------	--

87	Privacy	§164.530(h)	Waiver of rights
----	---------	-------------	------------------

88

Privacy

§164.530(i)

Policies and Procedures

89

Privacy

§164.530(j)

Documentation

90

Security

§164.306(a)

General Requirements

91

Security

§164.306(b)

Flexibility of approach

92

Security

§164.308(a)

Security Management
Process

93

Security

§164.308(a)(1)(ii)(A)

Security Management
Process -- Risk Analysis

94

Security

§164.308(a)(1)(ii)(B)

Security Management
Process -- Risk
Management

95

Security

§164.308(a)(1)(ii)(C)

Security Management
Process – Sanction
Policy

96

Security

§164.308(a)(1)(ii)(D)

Security Management
Process --Information
System Activity Review

97

Security

§164.308(a)(2)

Assigned Security
Responsibility

98

Security

§164.308(a)(3)(i)

Workforce Security

99

Security

§164.308(a)(3)(ii)(A)

Workforce security --
Authorization and/or
Supervision

100

Security

§164.308(a)(3)(ii)(B)

Workforce security --
Workforce Clearance
Procedure

101

Security

§164.308(a)(3)(ii)(C)

Workforce security --
Establish Termination
Procedures

102

Security

§164.308(a)(4)(i)

Information Access
Management

103	Security	§164.308(a)(4)(ii)(A)	Information Access Management -- Isolating Healthcare Clearinghouse Functions
-----	----------	-----------------------	---

104	Security	§164.308(a)(4)(ii)(B)	Information Access Management -- Access Authorization
-----	----------	-----------------------	---

105

Security

§164.308(a)(4)(ii)(C)

Information Access
Management -- Access
Establishment and
Modification

106

Security

§164.308(a)(5)(i)

Security Awareness and
Training

107

Security

§164.308(a)(5)(ii)(A)

Security Awareness and
Training -- Security
Reminders

108

Security

§164.308(a)(5)(ii)(B)

Security Awareness,
Training, and Tools --
Protection from
Malicious Software

109

Security

§164.308(a)(5)(ii)(C)

Security Awareness,
Training, and Tools --
Log-in Monitoring

110

Security

§164.308(a)(5)(ii)(D)

Security Awareness,
Training, and Tools --
Password Management

111

Security

§164.308(a)(6)(i)

Security Incident
Procedures

112

Security

§164.308(a)(6)(ii)

Security Incident
Procedures --
Response and
Reporting

113

Security

§164.308(a)(7)(i)

Contingency Plan

114

Security

§164.308(a)(7)(ii)(A)

Contingency Plan –
Data Backup Plan

115

Security

§164.308(a)(7)(ii)(B)

Contingency Plan
–Disaster Recovery
Plan

116

Security

§164.308(a)(7)(ii)(C)

Contingency Plan --
Emergency Mode
Operation Plan

117

Security

§164.308(a)(7)(ii)(D)

Contingency Plan --
Testing and Revision
Procedure

118

Security

§164.308(a)(7)(ii)(A)

Contingency Plan --
Application and Data
Criticality Analysis

119

Security

§164.308(a) (8)

Evaluation

120

Security

§164.308(b)(1)

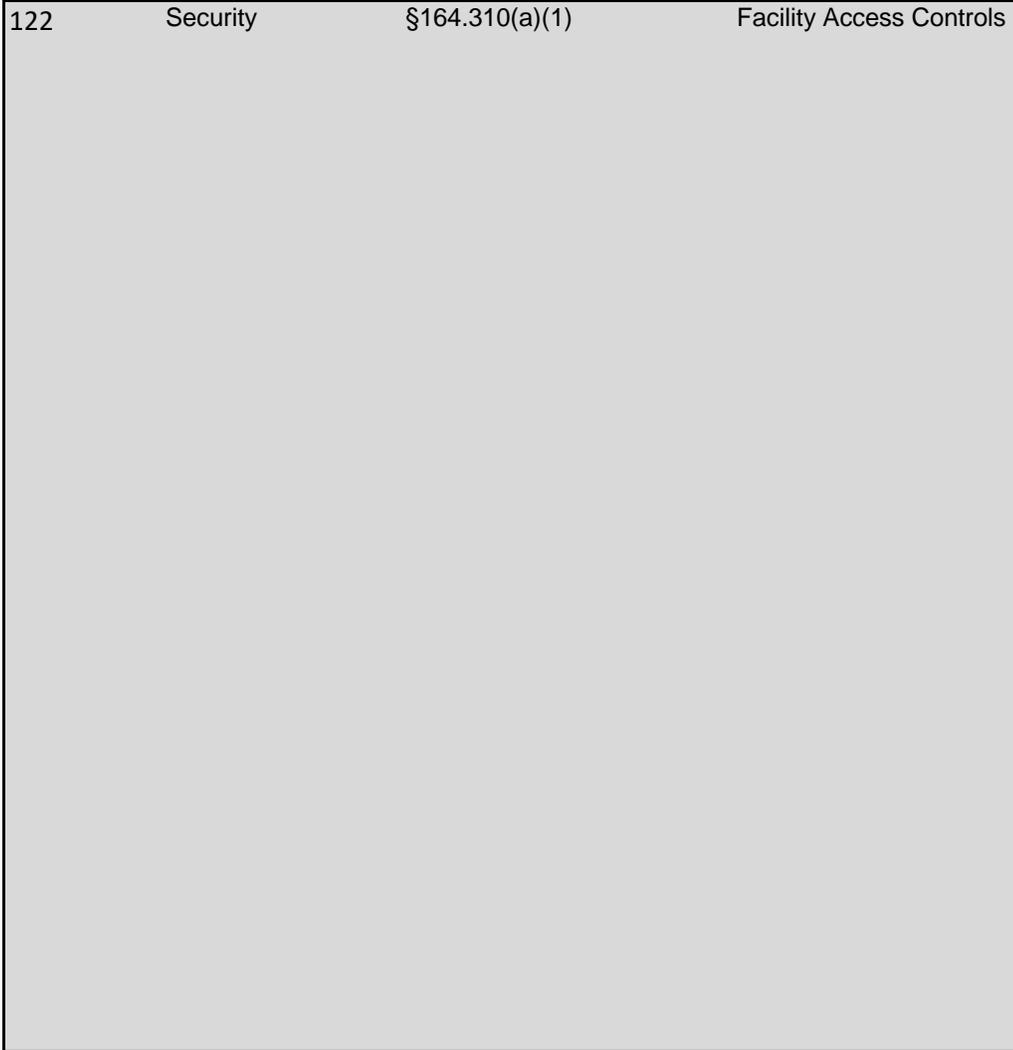
Business Associate
Contracts and Other
Arrangements

121

Security

§164.308(b)(3)

Business Associate
Contracts and Other
Arrangements -- Written
Contract or Other
Arrangement



123

Security

§164.310(a)(2)(i)

Facility Access Controls
-- Contingency
Operations

124

Security

§164.310(a)(2)(ii)

Facility Access Controls
-- Facility Security Plan



125

Security

§164.310(a)(2)(iii)

Facility Access Controls
-- Access Control and
Validation Procedures

126

Security

§164.310(a)(2)(iv)

Facility Access Controls
-- Maintain Maintenance
Records

127

Security

§164.310(b)

Workstation Use

128

Security

§164.310(c)

Workstation Security

129

Security

§164.310(d)(1)

Device and Media
Controls

130

Security

§164.310(d)(2)(i)

Device and Media
Controls -- Disposal

131

Security

§164.310(d)(2)(ii)

Device and Media
Controls -- Media Re-
use

132

Security

§164.310(d)(2)(iii)

Device and Media
Controls --
Accountability

133

Security

§164.310(d)(2)(iv)

Device and Media
Controls -- Data Backup
and Storage Procedures

134

Security

§164.312(a)(1)

Access Control

135

Security

§164.312(a)(2)(i)

Access Control --
Unique User
Identification

136

Security

§164.312(a)(2)(ii)

Access Control --
Emergency Access
Procedure

137

Security

§164.312(a)(2)(iii)

Access Control --
Automatic Logoff

138

Security

§164.312(a)(2)(iv)

Access Control --
Encryption and
Decryption

139

Security

§164.312(b)

Audit Controls

140

Security

§164.312(c)(1)

Integrity

141

Security

§164.312(c)(2)

Integrity -- Mechanism
to Authenticate ePHI

142

Security

§164.312(d)

Person or Entity
Authentication

143

Security

§164.312(e)(1)

Transmission

144

Security

§164.312(e)(2)(i)

Transmission Security --
Integrity Controls

145

Security

§164.312(e)(2)(ii)

Transmission Security --
Encryption

146

Security

164.314(a)(1)

Business Associate
Contracts or Other
Arrangements

147	Security	164.314(a)(2)(i)(A)	Business associate contracts
148	Security	164.314(a)(2)(i)(B)	Business associate contracts.
149	Security	164.314(a)(2)(i)(C)	Business associate contracts.
150	Security	164.314(a)(2)(ii)	Other Arrangements
151	Security	164.314(a)(2)(iii)	Business associate contracts with subcontractors

152	Security	164.314(b)(1)	Requirements for Group Health Plans
153	Security	164.314(b)(2)(i)	Group Health Plan Implementation Specification
154	Security	164.314(b)(2)(ii)	Group Health Plan Implementation Specification
155	Security	164.314(b)(2)(iii)	Group Health Plan Implementation Specification
156	Security	164.314(b)(2)(iv)	Group Health Plan Implementation Specification

157	Security	§164.316(a)	Policies and Procedures
-----	----------	-------------	-------------------------

158	Security	§164.316(b)(1)	Documentation
-----	----------	----------------	---------------

159	Security	§164.316(b)(2) (i)	Documentation – Time Limit
-----	----------	--------------------	-------------------------------

160	Security	§164.316(b)(2) (ii)	Documentation- Availability
-----	----------	---------------------	--------------------------------

161	Security	§164.316(b)(2) (iii)	Documentation – Updates
162	Breach	§164.414(a)	Administrative Requirements
163	Breach	§164.530(b)	Training
164	Breach	§164.530(d)	Complaints
165	Breach	§164.530(e)	Sanctions

166	Breach	§164.530(g)	Refraining from Retaliatory Acts
167	Breach	§164.530(h)	Waiver of Rights
168	Breach	§164.530(i)	Policies and Procedures
169	Breach	§164.530(j)	Documentation

170

Breach

§164.402

Definitions: Breach –
Risk Assessment

171

Breach

§164.402

Definitions: Breach -
exceptions

Unsecured PHI

172	Breach	§164.404(a)	Notice to Individuals
-----	--------	-------------	-----------------------

173	Breach	§164.404(b)	Timeliness of Notification
-----	--------	-------------	----------------------------

174	Breach	§164.404(c)(1)	Content of Notification
-----	--------	----------------	-------------------------

175

Breach

§164.404(d)

Methods of Notification

176

Breach

§164.406

Notification to the Media

177

Breach

§164.408

Notification to the
Secretary

178

Breach

§164.410

Notification by a
Business Associate

179	Breach	§164.412	Law Enforcement Delay
-----	--------	----------	-----------------------

180	Breach	§164.414(b)	Burden of Proof
-----	--------	-------------	-----------------

Established Performance Criteria

§ 164.502(a)(5)(i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan: (A) Except as provided in paragraph (a)(5)(i)(B) of this section: (1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and (4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. (B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

From § 160.103 Definitions.

Genetic information means: (1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about: (i) The individual's genetic tests; (ii) The genetic tests of family members of the individual; (iii) The manifestation of a disease or disorder in family members of such individual; or (iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual. (2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

(i) A fetus carried by the individual or family member who is a pregnant woman; and (ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology. (3) Genetic information excludes information about the sex or age of any individual. (ii) Genetic services means: (1) A genetic test; (2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or (3) Genetic education. Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

§164.502(f) Standard: Deceased individuals: A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

From § 160.103 Definitions.

Protected health information means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, [...]

(2) Protected health information excludes individually identifiable health information: [...] (iv) Regarding a person who has been deceased for more than 50 years.

§164.502(g)(1) Standard: Personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

§164.502(g)(2) Implementation specification: adults and emancipated minors: If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

§164.502(g)(3)(i) Implementation specification: unemancipated minors: If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or

(C) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

§164.502(g)(3)(ii) - Notwithstanding the provisions of paragraph (g)(3)(i) of this section:

(A) If, and to the extent permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or in accordance with §164.524 provide access to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis;

(B) If, and to the extent prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or in accordance with §164.524 provide access to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; and

(C) Where the parent, guardian, or other person acting in loco parentis, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or

§164.502(h) Standard: Confidential communications: A covered health care provider or health plan must comply with the applicable requirements of §164.522(b) in communicating protected health information.

§164.522(b)(1) Standard: Confidential communications requirements: (i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations. (ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

§164.522(b)(2) Implementation specifications: Conditions on providing confidential communications: (i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing. (ii) A covered entity may condition the provision of a reasonable accommodation on: (A) When appropriate, information as to how payment, if any, will be handled; and (B) Specification of an alternative address or other method of contact. (iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis. (iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

§164.502(i) Standard: Uses and disclosures consistent with notice: A covered entity that is required by §164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by §164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in §164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

§164.502(j)(1) Disclosures by whistleblowers: A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

- (i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and
- (ii) The disclosure is to:
 - (A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or
 - (B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

§164.502(j)(2) - Disclosures by workforce members who are victims of a crime: A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

- (i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and
- (ii) The protected health information disclosed is limited to the information listed in §164.512(f)(2)(i).

§164.504(e)(1) Standard: Business associate contracts.

(i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) Implementation specifications: Business associate contracts. A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

(D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

§164.504(f)(1) Standard: Requirements for group health plans.

(i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart. (ii) Except as prohibited by § 164.502(a)(5)(i), the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for purposes of: (A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or (B) Modifying, amending, or terminating the group health plan. (iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan. (2) Implementation specifications: Requirements for plan documents. The plan documents of the group health plan must be amended to incorporate provisions to: (i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart. (ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to: (A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law; (B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information; (C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor; (D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware; (E) Make available protected health information in accordance with § 164.524; (F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526; (G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528; (H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart; (I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for

§164.506(a) - Uses and disclosures to carry out treatment, payment, or health care operations. Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) through (4) or that are prohibited under § 164.502(a)(5)(i), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

§164.506(b) - Standard: Consent for uses and disclosures permitted.

§164.506(b)(1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

§164.506(b)(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under §164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.

§164.508(a)(1) Authorization required: General rule.

Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

§164.508(a)(2) Authorization required: Psychotherapy notes.

(i) Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

§164.508(a)(3) Authorization required: Marketing.

(i) Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

(A) A face-to-face communication made by a covered entity to an individual; or (B) a promotional gift of nominal value provided by the covered entity.

(ii) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.

§164.508(a)(4) Authorization required: Sale of protected health information.

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart.

(ii) Such authorization must state that the disclosure will result in remuneration to the covered entity.

§164.508(b)(3) Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.

§164.508(b)(4) Prohibition on conditioning of authorizations. A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

- (i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;
- (ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:
 - (A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and
 - (B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and
- (iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party

§164.508(b)(6) Documentation. A covered entity must document and retain any signed authorization under this section as required by §164.530(j).

§164.508(c) Implementation specifications: Core elements and requirements. (1) Core elements. A valid authorization under this section must contain at least the following elements:

- (i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
- (ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
- (iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
- (iv) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- (v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.
- (vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

§164.508(c)(2) Required Statements. In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

- (i) The individual's right to revoke the authorization in writing and either:
- (ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization.
- (iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient can no longer be protected by this subpart.

§164.508(c)(3) The authorization must be written in plain language.

§164.508(c)(4) If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

§164.510(a) Standard: Use and disclosure for facility directories. (1) Permitted uses and disclosure. Except when an objection is expressed in accordance with paragraph (a)(2) or (3) of this section, a covered health care provider may:

- (i) Use the following protected health information to maintain a directory of individuals in its facility:
 - (A) The individual's name;
 - (B) The individual's location in the covered health care provider's facility;
 - (C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and
 - (D) The individual's religious affiliation; and
- (ii) Use or disclose for directory purposes such information:
 - (A) To member of the clergy; or
 - (B) Except for religious affiliation, to other persons who ask for the individual by name.

(2) Opportunity to object. A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.

§164.510(a)(3) Emergency circumstances. (i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is: (A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and (B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.

§164.510(b) Standard: Uses and disclosures for involvement in the individual's care and notification purposes

(1) Permitted uses and disclosures. (i) A covered entity may, in accordance with paragraphs (b)(2), (b)(3), or (b)(5) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable.

§164.510(b) Standard: Uses and disclosures for involvement in the individual's care and notification purposes

(2) Uses and disclosures with the individual present. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

- (i) Obtains the individual's agreement;
- (ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
- (iii) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

§164.510(b)(3) Limited uses and disclosures when the individual is not present. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on

§164.510(b) Standard: Uses and disclosures for involvement in the individual's care and notification purposes (4) Uses and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3) or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the

164.510(b) Standard: Uses and disclosures for involvement in the individual's care and notification purposes (5) Uses and disclosures when the individual is deceased. If the individual is deceased, a covered entity may disclose to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

§164.512(a)(1) - A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies and is limited to the relevant requirements of such law.

§164.512(a)(2) - A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

§164.512(b) Standard: Uses and disclosures for public health activities.

(1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations; (B) To track FDA-regulated products; (C) To enable product recalls, repairs, or replacement, or look back (including locating and notifying individuals who have received products that have been, withdrawn, or are the subject of look back); or (D) To conduct post marketing surveillance; (iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer:

(1) To conduct an evaluation relating to medical surveillance of the workplace; or

(2) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

§164.512(c) Standard: Disclosures about victims of abuse, neglect or domestic violence

(1) Permitted disclosures. Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence: (i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements

§164.512(d) Standard: Uses and disclosures for health oversight activities

(1) Permitted disclosures. A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

- (i) The health care system;
- (ii) Government benefit programs for which health information is relevant to beneficiary eligibility;
- (iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
- (iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

§164.512(d)(2) Exception to health oversight activities. For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

- (i) The receipts of health care;
- (ii) A claim for public benefits related to health; or
- (iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

§164.512(d)(3) Joint activities or investigations. Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.

§164.512(d)(4) Permitted uses. If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.

§164.512(e)(1) Permitted disclosures. A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The party requesting such information has made a good faith attempts to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and

(1) No objections were filed; or

(2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(iv) For the purpose of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurance from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The parties to the dispute given rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over and dispute; or

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

(v) For purpose of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court of an administrative tribunal stipulation by the parties to the litigation or administrative proceeding that:

§164.512(f) Standard: Disclosures for law enforcement purposes. A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) Permitted disclosures: Pursuant to process and as otherwise required by law. A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demands, or similar process authorized under law, provided that:

(1) The information sought is relevant and material to a legitimate law enforcement inquiry;

(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(3) De-identified information could not reasonably be used.

§164.512(f)(2) Permitted disclosures: Limited information for identification and location purposes. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purpose of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of blood fluids or tissue.

§164.512(f)(3) Permitted disclosure: Victims of a crime. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:

(i) The individual agrees to the disclosure; or

(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interest of the individual as determined by the covered entity, in the exercise of professional judgment.

§164.512(f)(4) Permitted disclosure: Decedents. A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

§164.512(f)(5) Permitted disclosure: Crime on premises. A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

§164.512(f)(6) Permitted disclosure: Reporting crime in emergencies.

(i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to: (A) The commission and nature of a crime; (B) The location of such crime or of the victim(s) of such crime; and (C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, ~~paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement~~
§164.512(g) Standard: Uses and disclosures about decedents.

(1) Coroners and medical examiners. A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

§164.512(g)(2) Funeral directors. A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

§164.512(h) Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes. A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

§164.512(i) Standard: Uses and disclosures for research purposes (1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(3) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) Reviews preparatory to research. The covered entity obtains from the researcher representations that:

(A) Uses or disclosures is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) Research on decedent's information. The covered entity obtains from the researchers:

(A) Representation that the use or disclosure sought is solely for research on the protected health information or decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

§164.512(i) Standard: Uses and disclosures for research purposes (2) Documentation of waiver approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

- (i) Identification of IRB or date of action - A statement identifying the institutional review board or privacy board and the date on which the alteration or waiver of authorization was approved;
- (ii) Waiver criteria - A statement that the institutional review board or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:
 - (A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
 - (1) An adequate plan to protect the Identifiers from improper use and disclosure;
 - (2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
 - (3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;
 - (B) The research could not practicably be conducted without the waiver or alteration; and
 - (C) The research could not practicably be conducted without access to and use of the protected health information.
- (iii) Protected health information needed - A brief description of the protected health information for which use or access has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;
- (iv) Review and approval procedures - A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:
 - (A) An institutional review board must follow the requirements of the Common Rule, including the normal review procedures or the expedited review procedures: 7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45;
 - (B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(b)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board

§164.512(k) Standard: Uses and disclosures for specialized government functions.

- (1) Military and veterans activities
 - (i) Armed Forces personnel. A covered entity may use or disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the Federal Register the following information:
 - (A) Appropriate military command authorities; and
 - (B) The purposes for which the protected health information may be used or disclosed.
 - (ii) Separation or discharge from military service. A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.
 - (iii) Veterans. A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.
 - (iv) Foreign military personnel. A covered entity may use or disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the Federal Register pursuant to paragraph (k)(1)(i) of this section.
-

§164.512(k)(2) National security and intelligence activities. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).

§164.512(k)(3) Protective services for the President and others. A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

§164.512(k)(4) Medical suitability determinations.- A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

- (i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698;
- (ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or
- (iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

§164.512(k)(5) Correctional institutions and other law enforcement custodial situations.

(i) Permitted disclosures. A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for: (A) The provision of health care to such individuals; (B) The health and safety of such individual or other inmates; (C) The health and safety of the officers or employees of or others at the correctional institution; (D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another; (E) Law enforcement on the premises of the correctional institution; or (F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) Permitted uses. A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) No application after release. For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) Covered entities that are government programs providing public benefits.

(i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

§164.512(l) Standard: Disclosures for workers' compensation. A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

§164.514 (b) Implementation specifications: Requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of any experience with generally accepted statistical scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify and individual who is a subject for the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current available data from the Bureau of the Census;

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into single category of age 90 or older;

(D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger voice prints;

(Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

§164.514(c) Implementation specifications: Re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity,

(b) Standard: Minimum necessary

(1) Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) Minimum necessary does not apply. This requirement does not apply to:

- (i) Disclosures to or requests by a health care provider for treatment;
- (ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;
- (iii) Uses or disclosures made pursuant to an authorization under § 164.508;
- (iv) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;
- (v) Uses or disclosures that are required by law, as described by § 164.512(a); and
- (vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

§164.514(d)(2) Implementation specifications: Minimum necessary uses of protected health information.

(i) A covered entity must identify: (A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and (B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

§164.514(d)(3) Implementation specification: Minimum necessary disclosures of protected health information.

(i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must: (A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and (B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when: (A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s); (B) The information is requested by another covered entity; (C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or (D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.

§164.514(d)(4) Implementation specifications: Minimum necessary requests for protected health information. (i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

§164.514(d)(5) Implementation specification: Other content requirement. For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

§164.514(e)(1) Standard: Limited data set. A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

§164.514(e)(2) Implementation specification: Limited data set: A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images.

§164.514(e)(3) Implementation specification: Permitted purposes for uses and disclosures. (i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.

(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

§164.514(e)(4) Implementation specifications: Data use agreement (i) Agreement required. A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.

(ii) Contents. A data use agreement between the covered entity and the limited data set recipient must: (A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity; (B) Establish who is permitted to use or receive the limited data set; and (C) Provide that the limited data set recipient will: (1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law; (2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement; (3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware; (4) Ensure that any agents to whom it provides the limited

§164.514(f) Fundraising communications.

(1) Standard: Uses and disclosures for fundraising. Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508: (i) Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth; (ii) Dates of health care provided to an individual; (iii) Department of service information; (iv) Treating physician; (v) Outcome information; and (vi) Health insurance status.

(2) Implementation specifications: Fundraising requirements.

(i) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by §164.520(b)(1)(iii)(A) is included in the covered entity's notice of privacy practices. (ii) With each fundraising communication made to an individual under this paragraph, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost. (iii) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications. (iv) A covered entity may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(2)(ii) of this section. (v) A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

§164.514(g) Standard: Uses and disclosures for underwriting and related purposes. If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose or as may be required by law, subject to the prohibition at § 164.502(a)(5)(i) with respect to genetic information included in the protected health information.

§ 164.502(a)(5)(i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:

(A) Except as provided in paragraph (a)(5)(i)(B) of this section: (1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and (4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

(B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

From § 160.103 Definitions.

Genetic information means: (1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about: (i) The individual's genetic tests; (ii) The genetic tests of family members of the individual; (iii) The manifestation of a disease or disorder in family members of such individual; or (iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual. (2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

(i) A fetus carried by the individual or family member who is a pregnant woman; and (ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology. (3) Genetic information excludes information about the sex or age of any individual.

(ii) Genetic services means: (1) A genetic test; (2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or (3) Genetic education. Genetic test means an analysis of human DNA, RNA, chromosomes,

§164.514(h)(1) Standard: Verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must: (i) Except with respect to disclosures under §164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and (ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) Implementation specifications: Verification.

(i) Conditions on disclosures. If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements. (A) The conditions in §164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met. (B) The documentation required by §164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with §164.512(i)(2)(i) and (v).

(ii) Identity of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official: (A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status; (B) If the request is in writing, the request is on the appropriate government letterhead; or (C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) Authority of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official: (A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; (B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) Exercise of professional judgment. The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with §164.510 or acts on a good faith belief in making a disclosure in accordance with §164.512(j).

§164.520(a)(1) Right to notice. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

§164.520(b)(1) Required elements. The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) Header. The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

(ii) Uses and disclosures. The notice must contain: (A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations. (B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization. (C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in §160.202 of this subchapter. (D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law. (E) A description of the types of uses and disclosures that require an authorization under §164.508(a)(2)– (a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by §164.508(b)(5).

(iii) Separate statements for certain uses or disclosures. If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement informing the individual of such activities, as applicable: (A) In accordance with §164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt out of receiving such communications; (B) In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan; or (C) If a covered entity that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, intends to use or disclose protected health information for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes.

(iv) Individual rights. The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows: (A) The right to request

§164.520(c) Implementation specifications: Provision of notice. A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

(1) Specific requirements for health plans. (i) A health plan must provide the notice: (A) no later than the compliance date for the health plan, to individuals then covered by the plan; (B) thereafter, at the time of enrollment, to individuals who are new enrollees.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(v) If there is a material change to the notice:

(A) A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.

(B) A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.

§164.520(c)(2) Specific requirements for certain covered health care providers. A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice:

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or

(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;

(iii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice.

(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

§164.520(c)(3) Specific requirements for electronic notice. (i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

§164.520(d) Implementation specifications: Joint notice by separate covered entities. Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that: (1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement. (2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity: (i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies; (ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and (iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement. (3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered

§164.520(e) Implementation specifications: Documentation. A covered entity must document compliance with the notice requirements, as required by §164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

§164.522(a)(1) Standard: Right of an individual to request restriction of uses and disclosures.

(i) A covered entity must permit an individual to request that the covered entity restrict: (A) uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and (B) disclosures permitted under §164.510(b).

(ii) Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§164.502(a)(2)(ii), 164.510(a) or 164.512.

(vi) A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:

(A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

(B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

§164.522(a)(2) Implementation specifications: Terminating a restriction. A covered entity may terminate a restriction, if :

(i) the individual agrees to or requests the termination in writing;

(ii) the individual orally agrees to the termination and the oral agreement is documented; or

(iii) the covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:

(A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and

(B) Only effective with respect to protected health information created or received after it has so informed the individual.

§164.522(a)(3) Implementation specification: Documentation. A covered entity must document a restriction in accordance with § 164.530(j) of this subchapter.

§164.522(b)(1) Standard: Confidential communications requirements.

(i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

§164.524(a) Standard: Access to protected health information. (1) Right of access. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to review and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for (i) psychotherapy notes; and (ii) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

§164.524(b) Implementation specifications: Requests for access and timely action. (1) Individual's request for access. The covered entity must permit an individual to request access to review or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

§164.524(b) Timely action by the covered entity. (i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows. (A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section. (B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section. (ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that: (A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; (B) The covered entity may have only one such extension of time for action on a request for access.

§164.524(c) Implementation specifications: Provision of access. If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(2) Form of access requested. (i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual. (ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and

§164.524(d) Implementation specifications: Denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements. (1) Making other information accessible. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

§164.524(d)(2) Denial. The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in §164.530(d) or to the Secretary pursuant to the procedures in §160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

§164.524(a) Standard: Access to protected health information. (2) Unreviewable grounds for denial. A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

- (i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.
- (ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
- (iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.
- (iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.
- (v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

§164.524(a) Standard: Access to protected health information. (3) Reviewable grounds for denial. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

- (i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
- (ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
- (iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

§164.524(a) Standard: Access to protected health information. (4) Review of a denial of access. If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

§164.524(d) Implementation specifications: Denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements: (4) Review of denial requested. If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial, to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

§164.524(e) Implementation specification: Documentation. A covered entity must document the following and retain the documentation as required by §164.530(j): (1) the designated record sets that are subject to access by individuals; and (2) the titles of the persons or offices responsible for receiving and processing requests for access by individuals.

§164.526(a) Standard: Right to amend. (1) Right to amend. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

§164.526(a) Standard: Right to amend. (2) Denial of amendment. A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request: (i) was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment; (ii) is not part of the designated record set; (iii) would not be available for reviewing under §164.524; or (iv) is accurate and complete.

§164.526(c) Implementation specifications: Accepting the amendment. If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) Making the amendment. The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) Informing the individual. In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of an agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) Informing others. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to: (i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and (ii) persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

§164.526(d) Implementation specifications: Denying the amendment. If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) Denial . The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain: (i) The basis for the denial, in accordance with paragraph (a)(2) of this section; (ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement; (iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and (iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(2) Statement of disagreement. The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) Rebuttal statement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) Recordkeeping. The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) Future disclosure. (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates. (ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section. (iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

§164.528(a) Right to an accounting of disclosures of protected health information.

(1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years to the date on which the accounting is requested, except for disclosures: (i) To carry out treatment, payment and health care operations as provided in §164.506; (ii) To individuals of protected health information about them as provided in §164.502; (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in §164.502; (iv) Pursuant to an authorization as provided in §164.508; (v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in §164.510; (vi) For national security or intelligence purposes as provided in §164.512(k)(2); (vii) To correctional institutions or law enforcement officials as provided in §164.512(k)(5); (viii) As part of a limited data set in accordance with §164.514(e); or (ix) That occurred prior to the compliance data for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required. (ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must: (A) Document the statement, including the identity of the agency or official making the statement; (B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and (C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

§164.528(b) Implementation specifications: Content of the accounting. The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure: (i) The date of the disclosure; (ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person; (iii) A brief description of the protected health information disclosed; and (iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, the accounting may, with respect to such multiple disclosures, provide: (i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period; (ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and (iii) The date of the last such disclosure during the accounting period.

(4)(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide: (A) The name of the protocol or other research activity; (B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records; (C) A brief description of the type of protected health information that was disclosed; (D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period; (E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and (F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity. (ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

§164.528(c) Implementation specifications: Provision of the accounting. (1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that: (A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and (B) The covered entity may have only one such extension of time for action on a request for an accounting.

§164.528(c)(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

§164.528(d) Implementation specification: Documentation. A covered entity must document the following and retain the documentation as required by §164.530(j): (1) the information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section; (2) the written accounting that is provided to the individual under this section; and (3) the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

(a)(1) Standard: Personnel designations.

(i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(2) Implementation specification: Personnel designations. A covered entity must document the personnel designations and maintain in written or electronic form for six years.

§164.530(b)(1) Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

(2) Implementation specifications: Training. (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows: (A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity; (B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and (C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section. (ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

§164.530(c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. (2)(i) Implementation specification: Safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

§164.530(d)(1) Standard: Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.

§164.530(d)(2) Implementation specification: Documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

§164.530(e)(1) Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.

(2) Implementation specification: Documentation. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

§164.530(f) Standard: Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

§164.530(g) Standard: Refraining from intimidating or retaliatory acts. A covered entity—

(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and (2) must refrain from intimidation and retaliation as provided in §160.316.

§164.530(h) Standard: Waiver of rights. A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

§164.530(i)(1) Standard: Policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) Standard: Changes to policies and procedures. (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D of this part. (ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or (iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) Implementation specification: Changes in law. Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) Implementation specifications: Changes to privacy practices stated in the notice. (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must: (A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart; (B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and (C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice. (ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that: (A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and (B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

§164.530(j)(1) Standard: Documentation. A covered entity must: (i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form; (ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and (iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation. (iv) Maintain documentation sufficient to meet its burden of proof under § 164.414(b).

(2) Implementation specification: Retention period. A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

§164.306(a): Covered entities and business associates must do the following:

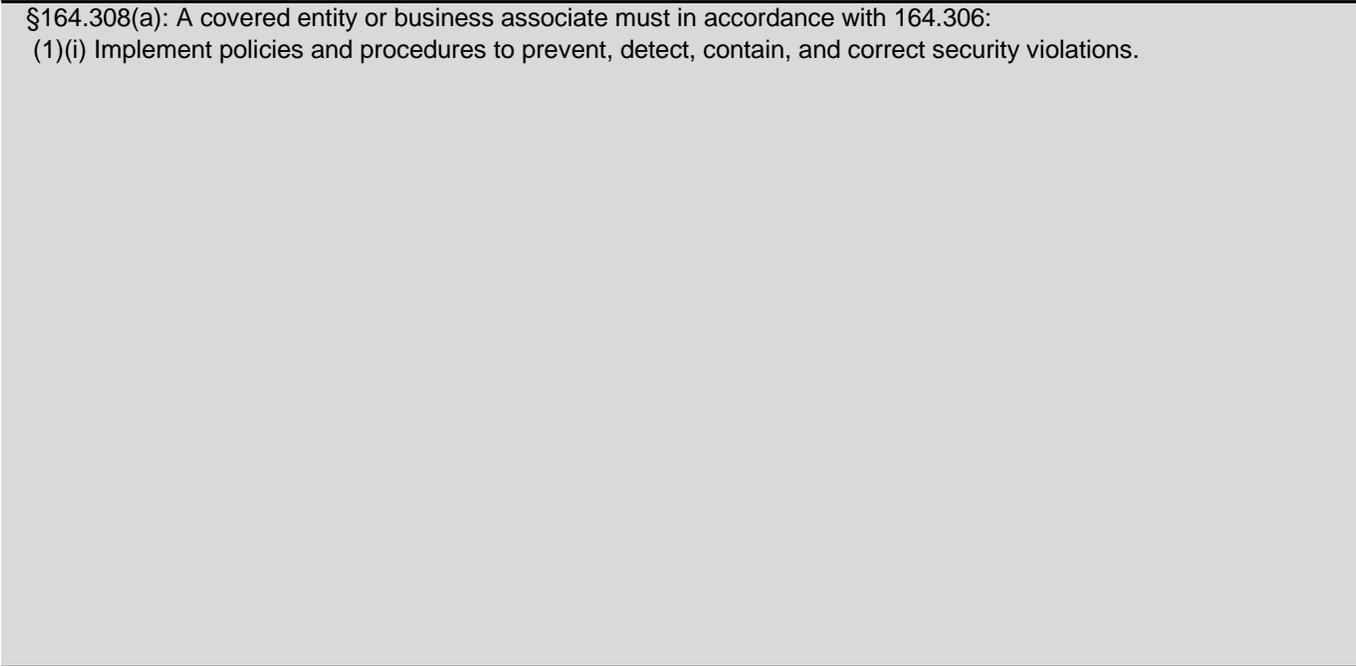
(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.

§164.306(b): Flexibility of approach.

(1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.

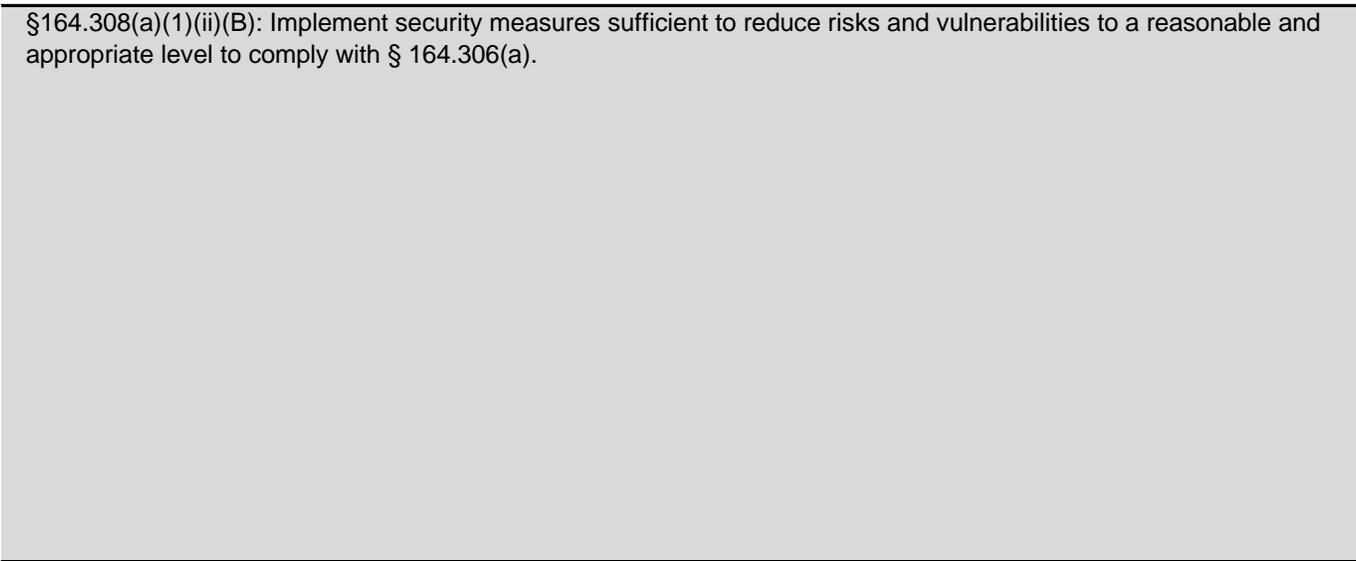
§164.308(a): A covered entity or business associate must in accordance with 164.306:

(1)(i) Implement policies and procedures to prevent, detect, contain, and correct security violations.



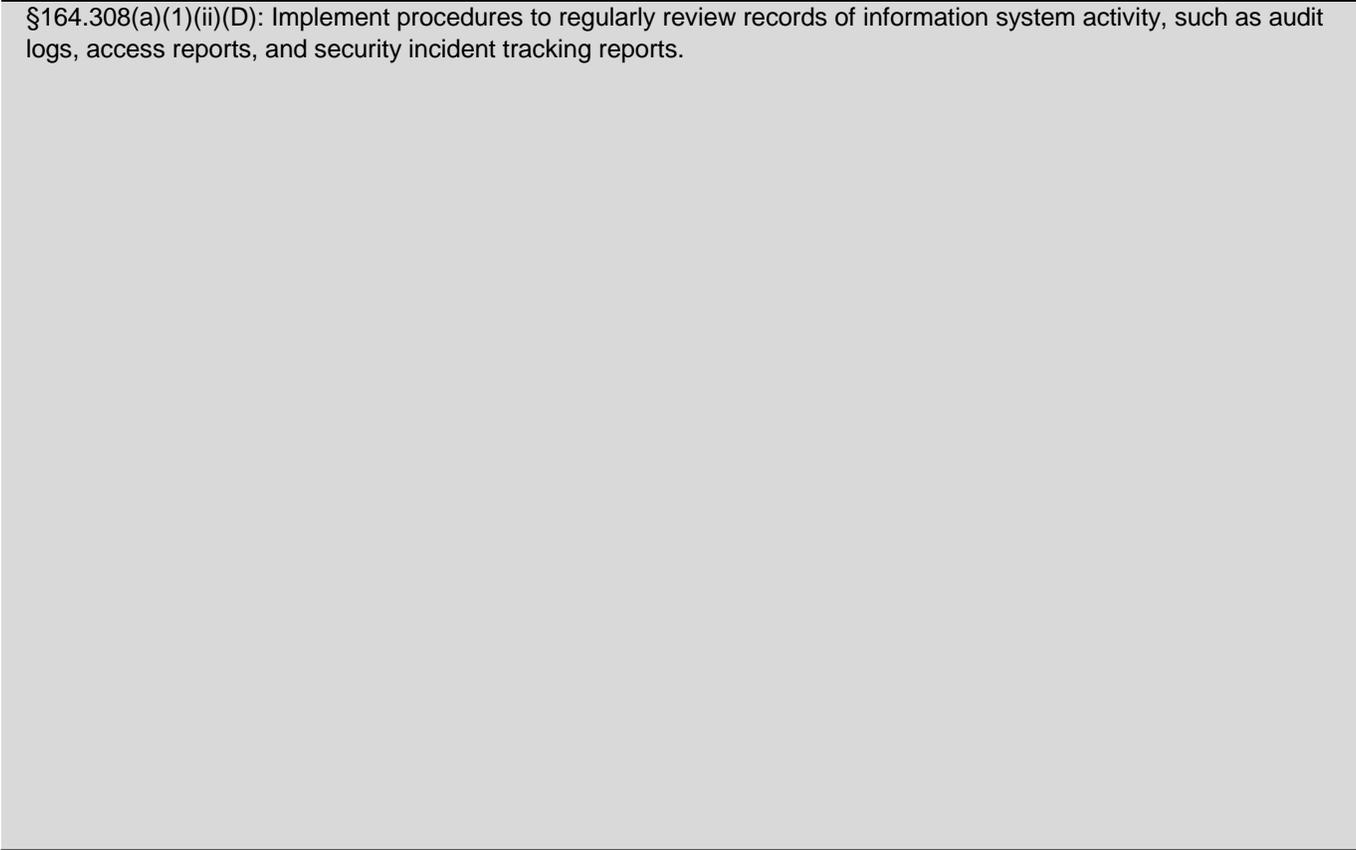
§164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

§164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).



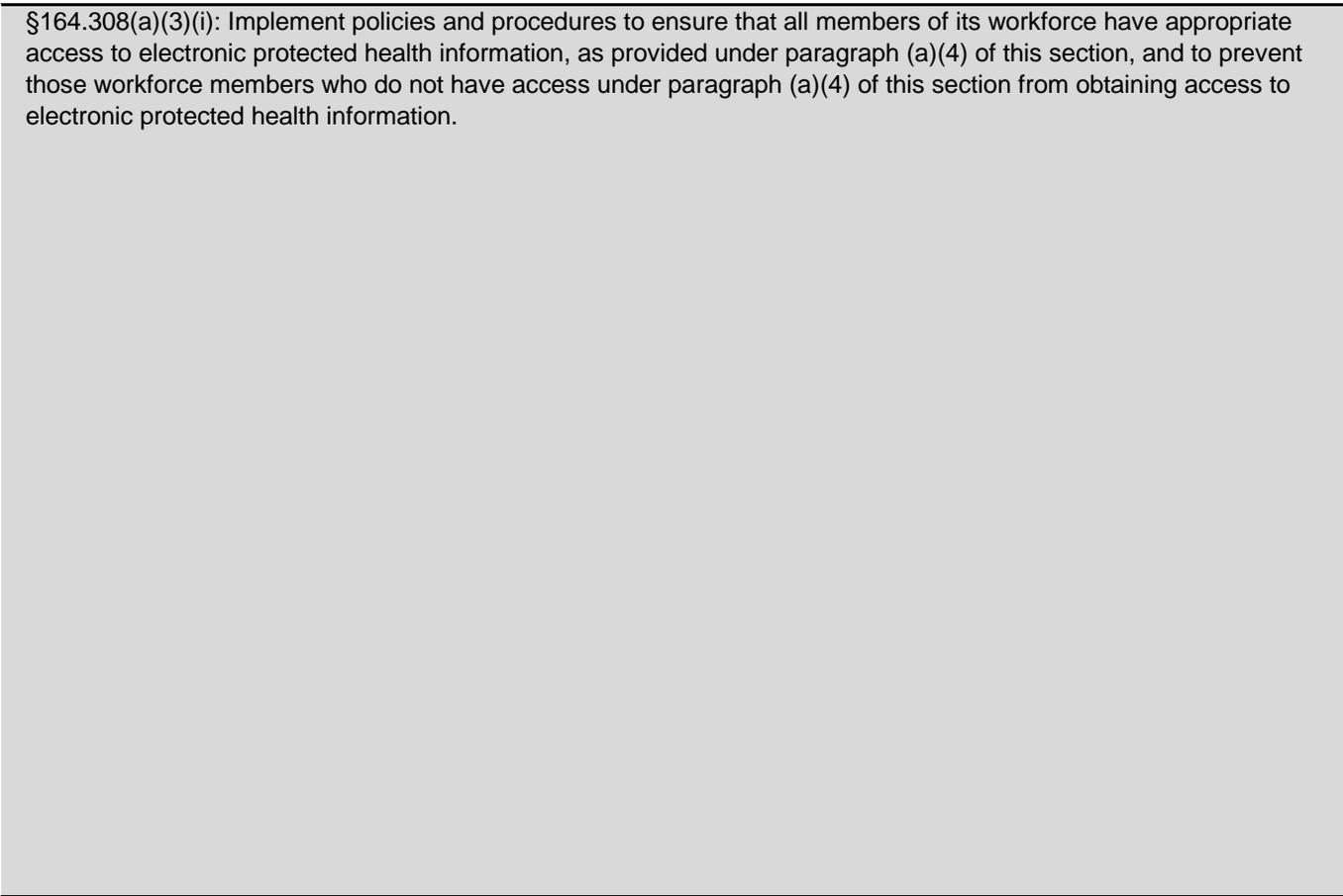
§164.308(a)(1)(ii)(C): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

§164.308(a)(1)(ii)(D): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.



§164.308(a)(2): Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

§164.308(a)(3)(i): Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

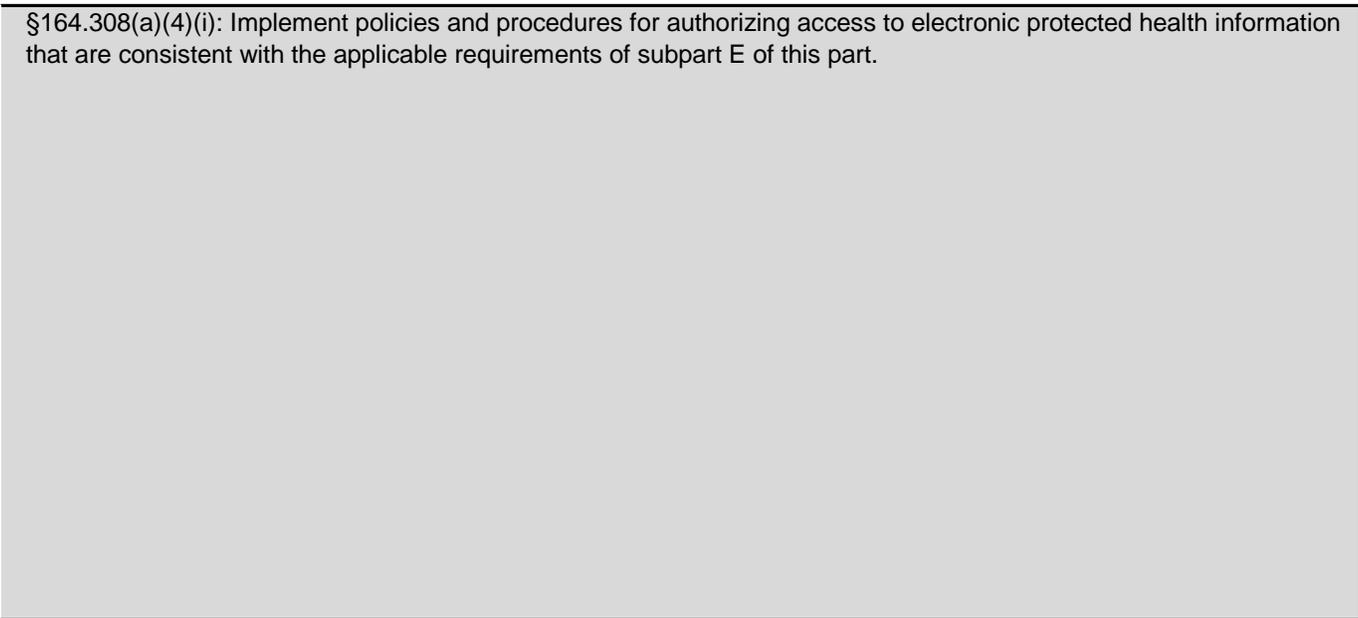


§164.308(a)(3)(ii)(A): Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

§164.308(a)(3)(ii)(B): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

§164.308(a)(3)(ii)(C): - Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).

§164.308(a)(4)(i): Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.



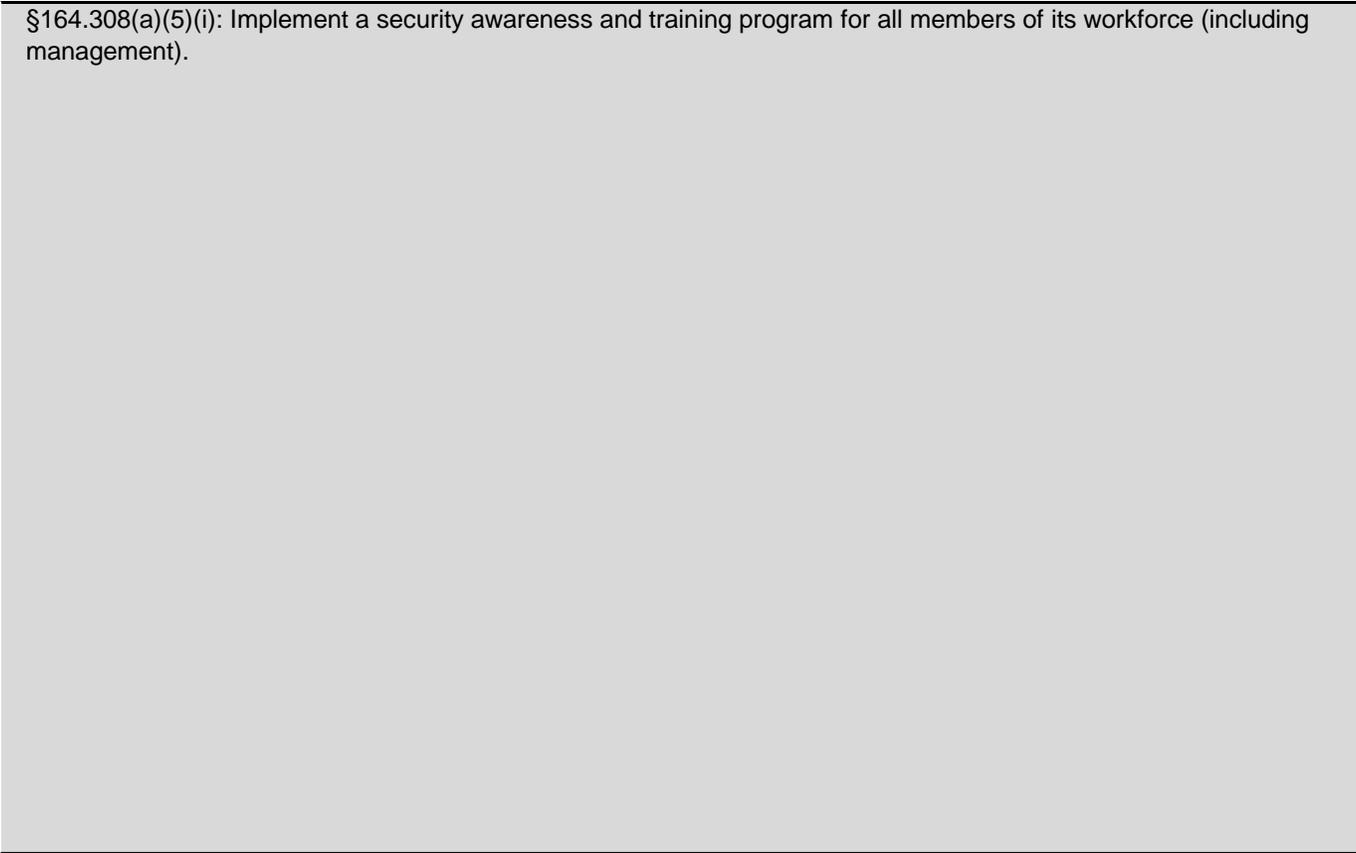
§164.308(a)(4)(ii)(A): If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

§164.308(a)(4)(ii)(B): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.



§164.308(a)(4)(ii)(C): Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

§164.308(a)(5)(i): Implement a security awareness and training program for all members of its workforce (including management).



§164.308(a)(5)(ii)(A): Periodic security updates.

§164.308(a)(5)(ii)(B): Procedures for guarding against, detecting, and reporting malicious software.



§164.308(a)(5)(ii)(C): Procedures for monitoring log-in attempts and reporting discrepancies.

§164.308(a)(5)(ii)(D): Procedures for creating, changing, and safeguarding passwords.



§164.308(a)(6)(i): Implement policies and procedures to address security incidents.

§164.308(a)(6)(ii): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

§164.308(a)(7)(i): Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

§164.308(a)(7)(ii)(A): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

§164.308(a)(7)(ii)(B): Establish (and implement as needed) procedures to restore any loss of data.

§164.308(a)(7)(ii)(C): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

§164.308(a)(7)(ii)(D): Implement procedures for periodic testing and revision of contingency plans.

§164.308(a)(7)(ii)(E): Assess the relative criticality of specific applications and data in support of other contingency plan components.

§164.308(a)(8): Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

§164.308(b)(1): A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

§164.308(b)(2): A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

§164.308(b)(3): Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

§164.310(a)(1): Implement policies and procedures to limit physical access to [an entity's] electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

§164.310(a)(2)(i): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

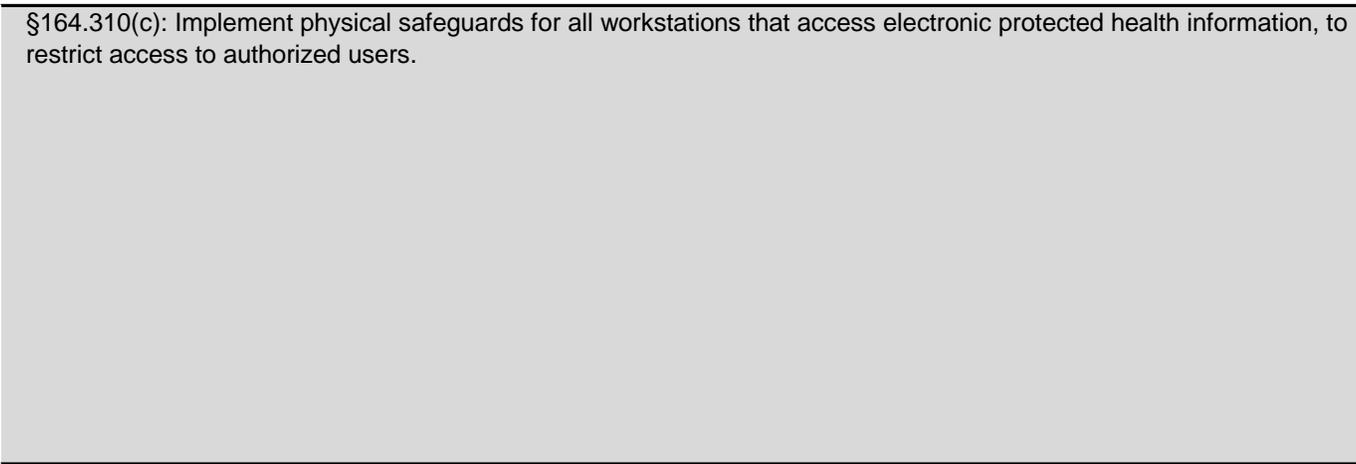
§164.310(a)(2)(ii): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

§164.310(a)(2)(iii): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision

§164.310(a)(2)(iv): Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

§164.310(b): Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

§164.310(c): Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.



§164.310(d)(1): Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility.

§164.310(d)(2)(i): Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored.

§164.310(d)(2)(ii): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

§164.310(d)(2)(iii): Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

§164.310(d)(2)(iv): Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

§164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

§164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.

§164.312(a)(2)(ii): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

§164.312(a)(2)(iii): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

§164.312(a)(2)(iv): Implement a mechanism to encrypt and decrypt electronic protected health information.

§164.312(b): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

§164.312(c)(1): Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

§164.312(c)(2): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

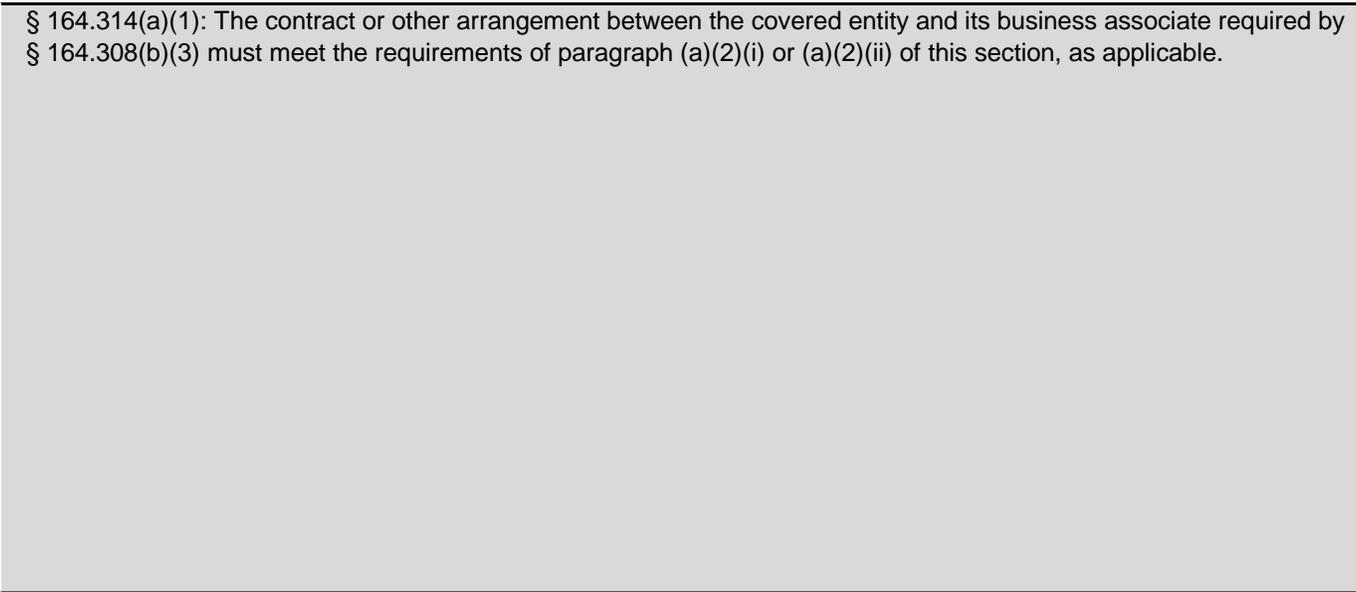
§164.312(d): Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

§164.312(e)(1): Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

§164.312(e)(2)(i): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

§164.312(e)(2)(ii): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

§ 164.314(a)(1): The contract or other arrangement between the covered entity and its business associate required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.



§ 164.314(a)(2)(i)(A): The contract must provide that the business associate will— (A) Comply with the applicable requirements of this subpart;

§ 164.314(a)(2)(i)(B):The contract must provide that the business associate will, in accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section

§ 164.314(a)(2)(i)(C): The contract must provide that the business associate will report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410

§ 164.314(a)(2)(ii): The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).

§ 164.314(a)(2)(iii): The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

§ 164.314(a)(b)(1): Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

§ 164.314(b)(2)(i): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.

§ 164.314(b)(2)(ii): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.

§ 164.314(b)(2)(iii): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.

§ 164.314(b)(2)(iv): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iv) Report to the group health plan any security incident of which it becomes aware.

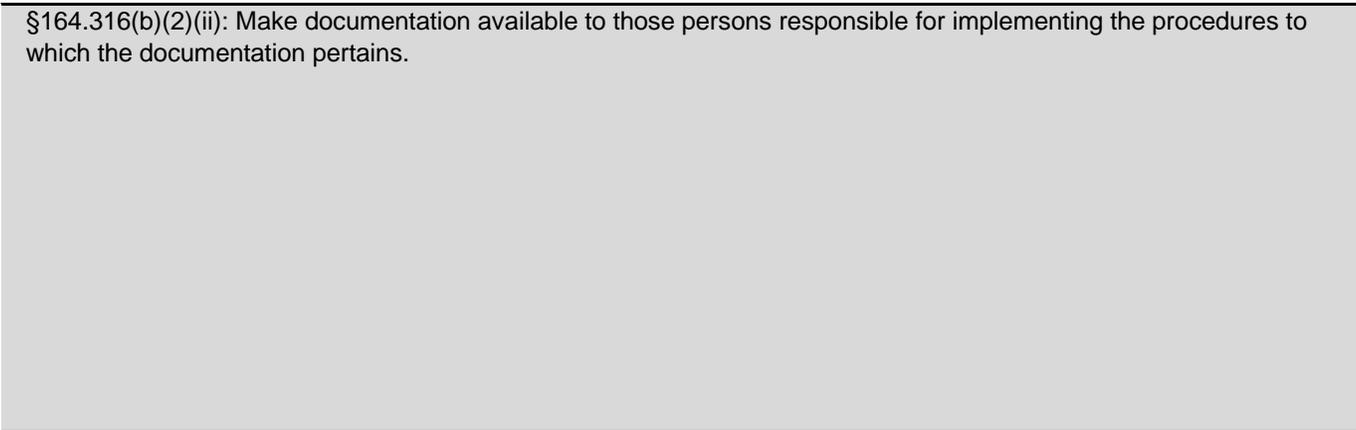
§164.316(a): Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

§164.316(b)(1):



§164.316(b)(2)(i): Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

§164.316(b)(2)(ii): Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.



§164.316(b)(2)(iii): Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

§164.414(a)

Administrative Requirements.

A covered entity is required to comply with the administrative requirements of §164.530(b), (d), (e), (g), (h), (i), and (j) with respect to 45 CFR Part 164, Subpart D ("the Breach Notification Rule").

[Training, complaints to the covered entity, sanctions, refraining from intimidating or retaliatory acts, waiver of rights, policies and procedures, and documentation]

§164.530(b)

Training.

All workforce members must receive training pertaining to the Breach Notification Rule.

164.530(d)

Complaints.

All covered entities must provide a process for individuals to complain about its compliance with the Breach Notification Rule.

164.530(e)

Sanctions.

All covered entities must sanction workforce members for failing to comply with the Breach Notification Rule.

164.530(g)

Refraining from Retaliatory Acts.

All covered entities must have policies and procedures in place to prohibit retaliatory acts.

164.530(h)

Waiver of Rights.

All covered entities must have policies and procedures in place to prohibit it from requiring an individual to waive any rights under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

164.530(i)

Policies and Procedures.

All covered entities must have policies and procedures that are consistent with the requirements of the Breach Notification Rule.

164.530(j)

Documentation.

All covered entities must have policies and procedures in place for maintaining documentation.

§164.402

Definitions: Breach - Risk Assessment.

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI.

(2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- (ii) The unauthorized person who used the PHI or to whom the disclosure was made;
- (iii) Whether the PHI was actually acquired or viewed; and
- (iv) The extent to which the risk to the PHI has been mitigated.

§164.402 - Definitions: Breach Exceptions - Unsecured PHI

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI.

(1) Breach excludes:

- (i) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
- (ii) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.
- (iii) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- (ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
- (iii) Whether the protected health information was actually acquired or viewed; and
- (iv) The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

§164.404(a)(1)

Notice to Individuals.

A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

§164.404(b)

Timeliness of Notifications.

Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

§164.404(c)(1)

Content of Notification.

The notification required by paragraph (a) of this section shall include, to the extent possible:

(A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(C) Any steps the individual should take to protect themselves from potential harm resulting from the breach;

(D) A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, Web site, or postal address.

(2) The notification required by paragraph (a) of this section shall be written in plain language.

§164.404(d)

Methods of Notification.

The notification required by paragraph (a) of this section shall be provided in the following form:

(1)(i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information becomes available.

(ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E) , written notification by first-class mail to either the next of kin or personal representative of the individual is required. The notification may be provided in one or more mailings as information is available.

(2) Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).

(i) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) Include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

(3) In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.

§164.406(a)

Notification to the Media.

For a breach of unsecured PHI involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.

(b) Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) The content of the notification required by paragraph (a) of this section shall meet the requirements of §164.404(c).

§164.408

Notification to the Secretary.

(a) A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.

(b) For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS Web site.

(c) For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS Web site.

§ 164.410

Notification by a Business Associate.

(a) Standard. (1) General Rule. A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach. (2) For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).

(b) Except as provided in § 164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c)(1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. (2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under § 164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

§164.412

Law Enforcement Delay.

If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

§164.414(b)

Burden of proof.

In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by the subpart or that the use or disclosure did not constitute a breach as defined at §164.402.

Audit Inquiry

Does the health plan use or disclose for underwriting purposes, "Genetic Information" as defined at § 160.103, including family history? Inquire of management.

Obtain and review all underwriting policies and procedures (for example, published and unpublished underwriting guidelines currently used by underwriting staff, including manuals and training materials). Evaluate whether the underwriting policies are consistent with the established performance criterion

Do the covered entity's policies and procedures protect the deceased individual's PHI consistent with the established performance criterion? Inquire of management.

Obtain and review policies and procedures regarding use and disclosure of deceased individuals' PHIs. Evaluate whether the policies and procedures are consistent with the established performance criterion.

Do the policies and procedures provide for the treatment of an authorized person as a personal representative?

Inquire of management how the entity recognizes personal representatives for an individual for compliance with HIPAA Rule requirements.

Obtain and review policies and procedures for the recognition and treatment of a personal representative. Evaluate whether the policies and procedures are consistent with the established performance criterion.

For example, do the policies and procedures address how the covered entity determines whether a person has authority to act on behalf of the individual? How do the policies and procedures address minors? The deceased?

Obtain and review a sample of personal representatives recognized by the entity. Evaluate whether the personal representative has been recognized and treated in a manner consistent with the established performance criterion and the entity established policies and procedures.

Obtain and review a sample of requests for persons to be recognized as personal representatives for individuals where the entity has not recognized the person as a personal representative. Evaluate whether the decision to not recognize the person as a personal representative was consistent with the established performance criterion and entity established policies and procedures. Evaluate whether the person has been treated consistent with the established performance criterion and the entity established policies and procedures.

How does the entity provide for and accommodate requests by individuals for confidential communications? Inquire of management how the entity handles requests for confidential communications by individuals.

Obtain and review policies and procedures regarding requests for confidential communications. Evaluate whether the policies and procedures are consistent with the established performance criterion.

Obtain and review a sample of confidential communications requests made by individuals. Evaluate whether the requests were evaluated and accepted or denied consistent with the established performance criterion and the entity established policies and procedures.

Obtain a review a sample of communications to individuals for which a confidential communication request was accepted. Evaluate whether the communication was conducted consistent with the established performance criterion and the entity established policies and procedures.

Are uses and disclosures made by the covered entity consistent with its notice of privacy practices?
Inquire of management whether uses and disclosures of PHI are consistent with the entity's notice of privacy practices.

Obtain and review policies and procedures regarding uses and disclosures. Evaluate whether the uses and disclosures of PHI are consistent with the entity's notice of privacy practices.

Are whistleblower policies and procedures consistent with the requirements of this performance criterion?

Obtain and review documentation of disclosures by a workforce member not otherwise permitted by the Privacy Rule that the entity determined to meet the requirements of this standard.

How has the covered entity ensured that disclosures by a workforce member related to his or her status as a victim of a crime are consistent with the rule?

Inquire of management how the entity identifies and treats disclosures of PHI by workforce members who are victims of a crime.

Obtain and review policies and procedures related to disclosures of PHI by workforce members who are victims of a crime. Evaluate whether disclosures are treated consistent with the established performance criterion and the entity established policies and procedures.

Does the covered entity enter into business associate contracts as required? Do these contracts contain all required elements? Inquire of management how the entity identifies and engages business associates.

Obtain and review policies and procedures related to the identification of business associates and the creation and establishment of business associate agreements. Evaluate whether the policies and procedures accurately identify business associates and establish business associate agreements consistent with the established performance criterion established performance criterion.

Technical Assistance: if available, review the entity's template business associate agreement and provide technical assistance as to its contents.

Obtain and review a sample of business associate agreements. Evaluate whether the agreements are consistent with the established performance criterion entity-established policies and procedures.

Inquire of management as to whether any business associate arrangements involved onward transfers of PHI to additional business associates and subcontractors. If yes, review a sample of business associate agreements between the covered entity and such business associates for provisions requiring subsequent BAs/subcontractors to provide adequate assurances.

Has the covered entity come into the knowledge of a pattern or practice of the business associate that constituted a material breach of violation of the BA's obligation? If so, obtain documentation of covered entity response and evaluate against the established performance criterion established performance criterion. Use of sampling procedures may be appropriate.

Obtain and review documentation of reports from the business associate to the covered entity of any uses or disclosures not provided for in its contract, and the covered entity response.

Do group health plan documents restrict the use and disclosure of PHI to the plan sponsor?

Obtain and evaluate group health plan documents to determine if they restrict the use and disclosure of PHI to the plan sponsor consistent with the established performance criterion

Do policies and procedures exist for the use or disclosure of PHI for treatment, payment, or health care operations?

Inquire of management.

Obtain and review policies and procedures regarding use or disclosure of PHI for treatment, payment, or health care operations.

Does the entity obtain the individual's consent for uses and disclosures?

Obtain samples of completed consents, if any, and patient intake materials and review to determine if its use is consistent with the established performance criterion.

What policies and procedures exist for obtaining a valid authorization when required?

Do policies and procedures exist to determine when authorization is required?

Obtain and review against the established performance criterion the policies and procedures for obtaining a valid authorization as required by the standard:

- Documentation of covered entity policy and procedures
- Documentation that a standard covered entity authorization, if any, is valid

Obtain and evaluate a sample of authorizations obtained to permit disclosures for consistency with the established performance criterion and entity-established policies and procedures.

For providers only: obtain and review all relevant patient intake forms for both inpatient and outpatient services, including consent and authorization forms, if any, to assess whether the provider's practice is to use a consent when an authorization would be required for any use or disclosure of information pursuant to the consent.

Does the covered entity use or disclose PHI for the purpose of research, conducts research, provides psychotherapy services, and uses compound authorizations?

Obtain and review a sample of used compound authorizations, if any.

Evaluate such authorizations in relation to the established performance criterion:

- Compound authorizations for the same research study
 - difference between conditioned and unconditioned components
 - Use or disclosure of psychotherapy notes and
 - Any other prohibition required under the established performance criterion
-

Does the covered entity condition treatment, payment, enrollment, or eligibility on receipt of an authorization? If so, does one of the limited exceptions apply?

Obtain and review policies and procedures related to seeking authorizations from individuals.
Obtain and review a sample of conditioned authorizations to assess whether the exceptions listed in the established performance criterion have been applied consistent with its requirements.

Does the covered entity document and retain signed, valid authorizations?

Obtain and review a sample of authorizations used as the basis for making uses and disclosures to determine if the authorizations are valid.

Does the entity maintain a directory of individuals in its facility?

Obtain and review policies and procedures that address determining if the individual has objected to uses and disclosures for facility directories and for documenting such determination.

Obtain and review a sample of the directory of individuals in the entity's facility that exists on the specified date and related documentation of individual objections. Evaluate the content against documentation of individual objections and against the listed content criteria.

Do policies and procedures exist to use or disclose PHI for the facility directory in emergency circumstances?

Obtain and review the policies and procedures used to disclose PHI for the facility directory due to an emergency circumstance.

What policies and procedures exist for disclosing PHI to family members, relatives, close personal friends, or other persons identified by the individual?

Obtain and review policies and procedures for such disclosures.

Under what circumstances does the covered entity disclose PHI to persons involved in the individual's care when the individual is present?

Obtain and review policies and procedures for determining or inferring individual agreement or lack of objection to disclosure of PHI with the individual present.

Do policies and procedures exist for disclosing only information relevant to the person's involvement in the individual's health care when the individual is not present and in related situations?

Obtain and review the policies and procedures used for disclosing only information relevant to the person's involvement with the individual's health care.

Do policies and procedures exist for disclosing PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts? Obtain and review policies and procedures in relation to such use or disclosure.

Does the covered entity disclose the PHI of deceased individuals in accordance with the established performance criterion?

Obtain and review policies and procedures related to documenting the individual's prior expressed preference and relationship of family members and other persons to the individual's care or payment for care, consistent with the established performance criterion.

Note: any information that would otherwise constitute PHI of a decedent under §160.201 ceases to be PHI 50 years after the death of the decedent.

Does the covered entity use and disclose PHI pursuant to requirements of other law? If so, are such uses and disclosures made consistent with the requirements of this performance criterion as well as the applicable requirements related to victims of abuse, neglect or domestic violence, pursuant to judicial and administrative proceedings and law enforcement purposes of this section? Obtain and review policies and procedures for uses and disclosures required by law.

Are policies and procedures in place that specify how the covered entity uses or discloses PHI for public health activities consistent with this standard?

Obtain and review policies and procedures in relation to the established performance criterion regarding permitted uses and disclosures for public health activities.

Obtain and review a sample of such uses and disclosures, to include uses and disclosures to an employer about an individual who is a member of the workforce of the employer, and determine whether all criteria were met.

How does the covered entity determine whether and how to make disclosures about victims of abuse, neglect, or domestic violence consistent with this standard?

Obtain and review policies and procedures. When and in what instances will the individual be notified that a disclosure has been or will be made?

Is PHI used or disclosed for health oversight activities consistent with the established performance criterion?

Obtain and review policies and procedures for using or disclosing PHI for health oversight activities.

Obtain a sample of disclosures made for this purpose and verify that the established performance criterion have been met.

Regarding §164.512(d)(4), is the covered entity also a health oversight agency? If so, is PHI used for health oversight activities conducted by the covered entity?

If yes, obtain and review policies and procedures for using PHI for health oversight activities conducted by the covered entity and determine whether they are consistent with the requirements of the established performance criterion.

Obtain a sample of uses made for this purpose and verify that the established performance criterion have been met.

Do policies and procedures exist related to making disclosures in the course of any judicial or administrative proceeding to limit such disclosures to those permitted by the established performance criterion?

Obtain and review policies and procedures related to disclosures of PHI made pursuant to judicial and administrative proceedings.

Obtain and review a sample of disclosures and the corresponding court orders, subpoenas, or discovery requests for judicial and administrative proceedings. Elements to consider include, but are not limited to, whether

the disclosure of PHI:

-Is in response to an order of a court or administrative tribunal

-Is in response to a subpoena, discovery request, or other lawful process.

Verify disclosure of PHI in the course of any judicial or administrative proceeding is appropriate.

Elements to consider should consist of the established performance criterion and include, but are not limited to:

-A court order requesting a response

-A subpoena.

Have disclosures made by the covered entity for law enforcement purposes been consistent with the performance criterion?

Obtain and review policies and procedures related to disclosures of PHI for law enforcement purposes against the established performance criterion.

Obtain and review a sample, as available, of disclosures and the corresponding court orders, subpoenas, discovery requests, etc., and determine if such disclosures are consistent with the established performance criterion.

Are disclosures made to law enforcement for identification and location purposes by the covered entity consistent with the limitations listed in the established performance criterion?

Obtain and review policies and procedures related to disclosures of PHI to law enforcement officials for identification and location purposes.

Obtain and review a sample of responses to law enforcement officials request for PHI for identification and location purposes and assess whether the disclosures were consistent with the established performance criterion.

Are policies and procedures consistent with the established performance criterion regarding the conditions in which the covered entity may disclose PHI of a possible victim of a crime in response to a law enforcement official's request?

Obtain and review policies and procedures related to such disclosures of PHI to law enforcement. If any, obtain and review a sample of responses to a law enforcement official's request to determine whether disclosure was made consistent with the established performance criterion.

Are policies and procedures in place to determine when it is permitted to disclose PHI to law enforcement about an individual who has died as a result of suspected criminal conduct?

Obtain and review policies and procedures related to disclosures of PHI to law enforcement officials that address the requirement.

Obtain and review documentation of such a disclosure, if available. Elements to consider include, but are not limited to, documentation of:

- Whether the entity exercised professional judgment
- Whether the entity believes in good faith that there was evidence of criminal conduct.

Are policies and procedures in place to determine when it is permitted to disclose PHI about an individual who may have committed a crime on the premises?

Determine whether policies and procedures related to disclosures of PHI to law enforcement officials address the established performance criterion.

Obtain and review a disclosure, if available. Elements to consider include, but are not limited to, documentation of:

- Whether the entity exercised professional judgment
 - Whether the entity believes in good faith that there was evidence of criminal conduct that occurred on its premises.
-

Are policies and procedures in place to determine what information about a medical emergency is necessary to disclose to alert law enforcement?

Determine whether policies and procedures related to disclosures of PHI to law enforcement officials address the established performance criterion.

Obtain and review a sample of such disclosures. Elements to consider include, but are not limited to, whether the disclosure:

- Indicates the commission and nature of the crime
- Includes the location of the crime or the victim(s) of the crime
- ~~-Includes the identity, description, and location of the perpetrator of the crime~~

Are policies and procedures consistent with the established performance criterion for disclosing PHI to (1) a coroner or medical examiner; and (2) a funeral director?

Obtain and review policies and procedures related to disclosures of PHI to coroners and medical examiners and funeral directors.

Obtain and review a sample of such disclosures. Elements to consider include, but are not limited to, whether the purpose of disclosure is:

- To identify a deceased person
- To determine the cause of death.
- Authorized by law.

Information elements to consider include, but are not limited to, whether the information disclosed is limited to:

- Name of deceased person
- Cause of death
- Compliance with such law.

Is the covered entity's process for disclosing PHI to organ procurement organizations or other entities engaged in the procurement consistent with the established performance criterion?

Obtain and review policies and procedures related to disclosures of PHI for purposes of cadaveric organ, eye, or tissue donation.

Obtain and review a sample of disclosures of PHI to organ procurement organizations to determine whether such disclosures are consistent with the policies and procedures and the established performance criterion.

Does the covered entity use or disclose PHI for research purposes? Inquire of management.

For entities that conduct research using or disclosing PHI, obtain and review related policies and procedures.

Elements to consider include, but are not limited to, how the entity:

- Obtains documentation that an alteration to a required authorization, or waiver of the authorization, has been approved by an IRB or appropriately configured privacy board
- Obtains from the researchers the required representations regarding reviews preparatory to research on decedents.

Verify if the entity obtained the necessary authorization and/or waiver to conduct the research.

Elements to consider include, but are not limited to:

- Board approval of a waiver of authorization
 - Whether the use or disclosure is solely to review PHI as necessary to prepare a research protocol
 - Representation that the use or disclosure is solely for research on the PHI of decedents.
-

Do policies and procedures exist to determine what documentation of approval or waiver is needed to permit a use or disclosure and to apply that determination?

Obtain and review policies and procedures against established performance criterion. Is the entity using or disclosing PHI consistent with requirements for documentation of a waiver approval? Verify that the documentation of any approval or waiver contains all the information necessary to permit a use or disclosure. Elements to consider include, but are not limited to:

- A statement identifying IRB and the date on which the alteration or waiver of authorization was approved
- Whether IRB determined that the alteration or waiver satisfied the criteria listed in the standard, including determination of no more than minimal risk to privacy, adequate plan to protect identifiers, adequate plan to destroy identifiers, etc.

Does the covered entity disclose PHI of individuals for military and veterans activities consistent with the established performance criterion?

Obtain and review policies and procedures related to disclosures of PHI for purposes of military and veterans' activities.

Obtain and review a list of uses and disclosures for military and veterans activities. Elements to consider are, 1) whether the entity is a component of the DoD, HSA; or VA; and 2) include whether the disclosure relates to:

- Armed force personnel
- Separated or discharged military service personnel
- A veteran
- Foreign military personnel.

. Elements to consider include, but are not limited to:

- Whether the activities deemed necessary by appropriate military command authorities
 - Whether the purpose is to determine the individual's eligibility for or entitlement to benefits under laws.
-

How would the covered entity respond to a request for PHI from Federal officials for intelligence and other national security activities?

Obtain and review policies and procedures related to disclosures of PHI for national security purposes.

How would the covered entity respond to a request for PHI from Federal officials for the provision of protective services or the conduct of certain investigations?

Obtain and review policies and procedures related to disclosures of PHI for protective services.

Is the covered entity a component of the Department of State?

If yes, does the covered entity have policies and procedures consistent with the established performance criterion to use and disclose PHI for the purposes described in the established performance criterion? Obtain and review such policies and procedures for consistency with the established performance criterion.

How does the covered entity determine whether to disclose PHI to a correctional institution or a law enforcement official with custody of an individual?

Are policies and procedures in place to determine whether a use or disclosure of PHI to a correctional institution or law enforcement official is permitted?

Obtain and review policies and procedures related to disclosures of PHI to correctional institutions or other law enforcement custodial situations for consistency with the established performance criterion.

Obtain and review a sample of documentation of disclosures to a correctional institution or law enforcement official; elements to consider include, but are not limited to, whether the disclosure is necessary for:

- The provision of health care to such individuals
- The health and safety of such individual or other inmates
- The health and safety of the officers or employees of or at the correctional institution
- The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another
- Law enforcement on the premises of the correctional institution
- The administration and maintenance of the safety, security, and good order of the correctional institution.

Is the covered entity a health plan that is a government program providing public benefits, or is it a government agency administering a government program providing public benefits?

If yes, does the covered entity have policies and procedures consistent with the established performance criterion in place to disclose PHI for the purposes listed? Obtain and review the policies and procedures.

Obtain and review a sample of such disclosures.

Are policies and procedures in place regarding disclosure of PHI for the purpose of workers' compensation, that are consistent with the established performance criterion?

Obtain and review policies and procedures related to disclosures of PHI for workers' compensation or other similar programs for consistency with the established performance criterion.

Obtain and review a sample of documentation of disclosures for the purpose of workers' compensation; elements to consider include, but are not limited to, whether the disclosure is authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

A covered entity may be , but is not required, to de-identify PHI.

Does the covered entity de-identify PHI consistent with the established performance criterion?

Obtain and review policies and procedures to determine whether they comply with the established performance criterion.

Refer to the de-identification guidance for assistance in these determinations:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html>

Has the covered entity implemented policies and procedures consistent with the requirements of the established performance criterion to identify need for and limit use of PHI?

Obtain and review policies and procedures for limiting access to PHI. Elements to consider include, but are not limited to:-

- Criteria for determining what level of access a person or class of persons will need
- Criteria for modifying, reviewing, or terminating an individual's access
- Efforts to limit access consistent with the needs and conditions described for each person or class of persons
- Whether the policies and procedures take into account access to both PHI and ePHI.

Obtain and review the access of a sample of workforce members with access to PHI for their corresponding job title and description to determine whether the access is consistent with the policies and procedures.

NOTE: The rule requires that the class/job functions that need to use or disclose PHI be determined and the information be limited to what is needed for that job classification.

Are policies and procedures in place to limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure?

Obtain and review policies and procedures related to minimum necessary disclosures and evaluate the content relative to the established performance criterion.

Obtain and review a sample of protocols for disclosures made on a routine and recurring basis and determine if such protocols limit to the PHI to what is reasonably necessary to achieve the purpose of the disclosure, as required by 514(d)(3).

Are policies and procedures in place to limit the PHI requested by the entity being audited to the amount minimally necessary to achieve the purpose of the disclosure?

Obtain and review policies and procedures related to minimum necessary requests and evaluate the content relative to the specified criteria.

Obtain and review a sample of requests made on a routine and recurring basis and determine if they are limited to the PHI reasonably necessary to achieve the purpose of the disclosure, as required by §164.514(d)(4).

Are policies and procedures in place to address uses, disclosures, or requests for an entire medical record?

Obtain and review policies and procedures related to minimum necessary uses, disclosures, or requests for an entire medical record for consistency with the established performance criterion.

Obtain and review a sample of use, disclosure, or request for an entire medical record and determine if it is limited to the PHI reasonably necessary to achieve the purpose of the use, disclosure, or request as required by §164.514(d)(5).

Are data use agreements in place between the covered entity and its limited data set recipients, if any?

Obtain and review policies and procedures and evaluate the content in relation to the established performance criterion to determine if data use agreements are in place between the covered entity and its limited data set recipients.

Obtain and review a sample data use agreement to determine if the agreements comply with the established performance criterion.

Obtain and review a sample limited data set to determine whether it complies with the established performance criterion.

Is the disclosure of PHI to a business associate or institutionally related foundation limited to the information set forth in the established performance criterion?

Obtain and review policies and procedures and notice of privacy practices and evaluate the content relative to the established performance criterion.

Obtain and review a sample of communications for fundraising purposes to determine if it contains a clear and conspicuous opportunity to opt-out of further fundraising communications or reference to a mechanism for opting out.

Obtain and review documentation that the policies and procedures are conveyed to the workforce.

Does the health plan have policies and procedures consistent with the established performance criterion addressing limitations on the use and disclosure of PHI received for underwriting and other purposes?

Obtain and review policies and procedures and evaluate the content relative to the established performance criterion. If health insurance or health benefits are not placed with the health plan, do the policies and procedures limit further use or disclosure for such purpose or as may be required by law?

See also § 164.502(a)(5)(i) of this document. Are policies and procedures in place restricting the health plan's uses and/or disclosures of PHI for underwriting purposes, subject to the prohibition with respect to genetic information in the PHI?

Are policies and procedures consistent with the established performance criterion in place to verify the identity of persons who request PHI?

Obtain and review policies and procedures regarding verification of the identity of individuals who request PHI.

Obtain and review sample documentation, consistent with the established performance criterion, of how the covered entity has verified the identity of several recent requestors of PHI. Such documentation could include a copy of or notation of the official credentials, a completed verification checklist, a copy of the request on official letterhead, etc.

Does the covered entity have a notice of privacy practices?

If yes, verify the current notice contains all the required elements.

- Header

164.502(a)(1) – Permitted uses and disclosures

Does the covered entity include in its notice a description of the following permitted uses and disclosures?

- To the individual
- For treatment, payment, or health care operations (with at least one example of a use and disclosure for each purpose)
- For public health and safety issues
- For research purposes
- To comply with the law
- To respond to organ and tissue donation requests
- To work with a medical examiner or funeral director
- To address workers' compensation, law enforcement and other government requests
- To respond to lawsuits and legal actions.

Pursuant to an agreement under, or as otherwise permitted by § 164.510 – Uses and disclosures requiring an opportunity to agree or object:

(i) For facility direct

(ii) For involvement in the individual's care and notification purposes.

64.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required

Does the covered entity include in its notice the following uses and disclosures for which an authorization or opportunity to agree or object is not required:

- As required by law
- For public health activities
- Disclosures about victims of abuse, neglect or domestic violence
- For health oversight activities
- Disclosures for judicial and administrative proceeding

Does the health plan provide its notice of privacy practices consistent with the established performance criterion?

Obtain and review the policies and procedures in place regarding the provision and posting of the notice of privacy practices.

Has the health plan provided the notice of privacy practices to individuals as required? For a sample of individuals, obtain and review documentation of when and how notices were provided.

As available, for example, as part of a standard mailing sent to new health plan members, review the notice of privacy practices provided to the selected individuals. Was the notice of privacy practices that was provided to the selected individuals the current notice of privacy practices for the time period in which the notice was provided?

Does a covered health care provider with direct treatment relationships with individuals provide its notice of privacy practices consistent with the established performance criterion?

Obtain and review the policies and procedures in place regarding the provision of the notice of privacy practices.

Obtain and review a sample of acknowledgement of receipt of the notice and of documentation showing a good faith effort was made when an acknowledgment could not be obtained.

Has the covered health care provider provided the notice of privacy practices to individuals as required? From sample of a population of individuals who were new patients/new individuals, obtain and review documentation to determine if the initial date of service corresponded with the date of the notice of privacy practices was received. If the dates do not correspond, determine if the initial service was an emergency situation or if there was another means or explanation.

Review documentation related to provision of notice to individuals who presented for emergency treatment.

Does a covered entity that maintains a web site prominently post its notice?

Does the covered entity implement policies and procedures, if any, to provide the notice electronically consistent with the standard?

Determine whether the entity maintains a web site. If so, observe the web site to determine if the notice of privacy practices is prominently displayed and available. An example of prominent posting of the notice would include a direct link from homepage with a clear description that the link is to the HIPAA Notice of Privacy Practices.

If the covered entity provides electronic notice (such as by linkage to a web page or e-mail), obtain and review the policies and procedures regarding the provision of the notice of privacy practices electronically and the process by which an individual can withdraw their request for receipt of electronic notice.

If the covered entity provides the notice of privacy practices by e-mail or other electronic form, obtain and review the documentation of the agreement with the individual to receive the notice via e-mail or other electronic form.

Inquire if covered entity has experienced failures when trying to provide the notice of privacy practices by e-mail. If the covered entity has experienced e-mail transmission failures, obtain and review its attempts to provide a paper copy of the notice via alternative means (e.g., mail).

For covered entities that participate in organized health care arrangement, does the entity use a joint notice of privacy practices?

If a joint notice is utilized, does the joint notice meet the specific additional criteria for a joint notice? Obtain and review the joint notice of privacy practices to determine whether it meets the established performance requirements.

Is the documentation of notice of privacy practices and the acknowledgement of receipt by individuals of the notice of privacy practices maintained in electronic or written form and retained for a period of 6 years?

Obtain and review policies and procedures to assess whether applicable documentation criteria for the notice are established and communicated to appropriate members of the workforce.

Obtain and review documentation (copies of all applicable notices and sample of acknowledgements) to determine if (1) the notice of privacy practices; and (2) (using a sample) acknowledgements for health care providers with direct treatment relationships with patients are maintained in electronic or written form and retained for a period of six years.

Does the covered entity have policies and procedures consistent with the established performance criterion to permit an individual to request that the entity restrict uses or disclosures of PHI for treatment, payment, and health care operations, and disclosures permitted pursuant to §164.510(b)?

Obtain and review policies and procedures against the established performance criterion.

Has the covered entity agreed to a restriction? If yes, obtain and review sample of documentation of each request and subsequent agreement to determine if restrictions are given effect.

Obtain and review all requests since September 23, 2013, for restrictions of information disclosed to a health plan in which the item or service has been paid for out of pocket in full. Obtain and review documentation of covered entity responses to determine if restrictions are given effect.

Are policies and procedures in place to terminate restrictions on the use and/or disclosure of PHI, consistent with the established performance criterion?

Obtain and review policies and procedures related to terminating restrictions of use and/or disclosure of PHI.

Has the covered entity terminated a restriction? If so, obtain and review a sample of documented terminated restriction to determine that the terminations are implemented consistent with the policies and procedures.

Does the covered entity, consistent with the established performance criterion, maintain documentation of restrictions in electronic or written form for a period of six years?

Obtain and review policies and procedures for documenting restriction requests and maintaining those documented restrictions.

Has the covered entity agreed to a restriction in the past six years? If yes, review the documentation required for P64, P65 for consistency with the established performance criterion.

Does the covered entity have policies and procedures in place to permit individuals to request alternative means or alternative locations to receive communications of PHI consistent with the established performance criterion? Does the covered entity have policies and procedures in place to accommodate such requests consistent with the established performance criterion?

Obtain and review policies and procedures describing how an individual may request to receive communications of PHI by alternative means and at alternative locations. Obtain and review documentation of sample requests and the covered entity response.

How does the covered entity enable the access rights of an individual? Inquire of management.

Obtain and review policies and procedures in place for individuals to request and obtain access to PHI and to determine whether they comply with the mandated criteria. Determine whether policies and procedures adequately address circumstances in which an access request is made for PHI that is not maintained by the covered entity, per 164.524(d)(3).

Obtain and review the notice of privacy practices. Identify whether an individual's right to access in a timely manner is correctly described in the notice.

Obtain and review access requests which were granted (and documentation of fulfillment, if any) and access requests which were denied.

- Verify that access was provided consistent with the policies and procedures
- Verify that requests for access were fulfilled in the form and format requested by the individual if the covered entity can readily produce the PHI in the requested form and format, including electronic format
- Determine whether response was made in a timely manner. (e.g., within 30 days of request receipt, unless extension provided consistent with 164.524(b)(2)(ii))
- Determine whether fee charged meets the reasonable cost based fee requirement of 164.524(c)(4)
- If the entity denied access to certain PHI, determine whether it provided access to other PHI requested by the individual that was not excluded, per §164.524(d)(1)
- For cases for which access was denied, assess whether the denials, and any reviews made pursuant to individual request, were consistent with the policies and procedures.

Inquire of management whether the covered entity has used a standard template or form letter for requesting access to protected health information. If the covered entity has used a standard template or form letter for access, obtain and review the document and determine whether it includes the requirements

Has the covered entity implemented policies and procedures that ensure that an individual receives a timely, written denial that contains all mandated elements?

Inquire of management.

Obtain and review policies and procedures to determine if they comply with the established performance criterion.

Obtain and review a sample of denied access requests.

Do policies and procedures exist that dictate the circumstances under which denials of requests for access are unreviewable?

Are policies and procedures in place regarding review of denials of access? Inquire of management.

Obtain and review policies and procedures to determine if the adopted process for the review of the denial of access complies with the mandated criteria.

Review documentation obtained for item 66 for consistency with these requirements

Do policies and procedures address request for and fulfillment of review of instances of access denial? Inquire of management.

Review policies and procedures to determine whether they comply with the established performance criterion. For example, does the entity have a process for an individual to request and receive a review of a denial of access by a licensed health care professional who did not participate in the original decision to deny the individual's request for access as set forth in §164.524(d)(4)? Does it provide prompt referral of denial for review by licensed health care professional not directly involved in the original denial, determination within a reasonable period of time, and prompt written notice to individual?

Review documentation obtained for item 66 for consistency with these requirements

Obtain and review documentation of the current designated record sets subject to access, as well as documentation for the last 6 years (as applicable).

Obtain and review policies and procedures to determine if a person or office is specified to process requests for access to PHI. Obtain the name or office specified for each year over the preceding 6-year documentation period.

Has the covered entity implemented policies and procedures consistent with the established performance criterion regarding an individual's right to amend their PHI in a designated record set?

Obtain and review policies and procedures allowing an individual the right to amend protected health information in a designated health record set.

Has the covered entity implemented policies and procedures consistent with the established performance criterion for determining grounds for denying requests?

Obtain and review documentation, including policies and procedures, of circumstances by which the entity has grounds for denial of amendment.

Verify grounds for denying request for amendment comply with the established performance criterion.

Does the covered entity have policies and procedures consistent with the established performance criterion for accepting requests for amendments?

Review policies and procedures for compliance with amendment criteria.

Obtain and review a sample of requests by individuals to amend their PHI or a record about the individual in a designated record set to determine whether they were addressed in accordance with the established performance criterion.

Has the covered entity implemented policies and procedures regarding provision of denial consistent with the established performance criterion?

Obtain and review entity policies and procedures.

Obtain and review a sample of denied requests for consistency with the established performance criterion.

Areas of review include timeliness; content of written denial; inclusion of statement of disagreement; provision of rebuttal statements to the individual; recordkeeping; inclusion of denial records when source information is disclosed.

Does the covered entity have policies and procedures consistent with the established performance criterion for implementing an individual's right to an accounting of disclosures of PHI?

Obtain and review policies and procedures in place to document and respond to a request for an accounting. Consider whether such documentation limits grounds for denials the ones listed in the established performance criterion.

Does the covered entity have policies and procedures consistent with the established performance criterion to provide an accounting that contains the content listed?

Obtain and review policies and procedures to determine whether the policies and procedures accurately provide for inclusion of the content listed in the established performance criterion.

Obtain and review a sample of requests for accounting and entity fulfillment of those requests to consider whether the accountings provided meet the established performance criterion.

Does the covered entity have policies and procedures consistent with the established performance criterion to provide an individual with a requested accounting of PHI with in the time and fee limitations specified?

Obtain and review policies and procedures to determine if the process to provide the individual with the requested accounting of PHI complies with the established performance criterion.

Review documentation obtained through items P75, P76 for consistency with this criteria.

Does the covered entity document requests for and fulfillment of accounting of disclosures consistent with the established performance criterion?

Obtain and review policies and procedures related to documentation of accountings of disclosures for consistency with the established performance criterion.

Review documentation provided for items 75, 76, to determine if the documentation complies with the established performance criterion.

Has the covered entity designated a privacy official and a contact person consistent with the established performance criterion?

Inquire of management (1) who is responsible for the development and implementation of the privacy policies and procedures; and(2) what person or office is designated to receive privacy complaints.

Obtain and review documentation to determine if the above items are maintained in electronic or written form and retained for a period of six years.

Does the covered entity train its work force and have a policies and procedures to ensure all members of the workforce receive necessary and appropriate training in a timely manner as provided for by the established performance criterion?

Obtain and review such policies and procedures. Areas to review include training each new member of the workforce within a reasonable period of time and each member whose functions are affected by a material change in policies or procedures.

From the population of new hires within the audit period, obtain and review a sample of documentation of necessary and appropriate training on the HIPAA Privacy Rule that has been provided and completed.

Obtain and review documentation that workforce members have been trained on material changes to policies and procedures required by the HITECH Act.

Has the covered entity implemented administrative, technical, and physical safeguards to protect all PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart? Does the covered entity reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure?

Obtain and review policies and procedures to determine if appropriate administrative, technical, and physical safeguards are in place.

Obtain and review documentation of specific safeguards in place from all three categories to reasonably protect the PHI. Such documentation may include, but is not limited to, policies and procedures, photographic or documentary documentation of physical and technical safeguards, and statements from privacy and security officials.

Does the covered entity have a process for individuals to make complaints, consistent with the requirements of the established performance criterion?

Obtain and review policies and procedures to determine how complaints are received, processed, and documented.

Has the covered entity documented all complaints received and their disposition consistent with the performance criteria?

Obtain and review a sample of documentation of complaints for consistency with the established performance criterion.

Does the covered entity apply appropriate sanctions against members of the workforce who fail to comply with the privacy policies and procedures of the entity or the Privacy Rule?

Obtain and review policies and procedures to determine if the entity has and applies sanctions consistent with the established performance criterion.

Obtain and review documentation of the application of sanctions to a sample of workforce members to determine whether appropriate sanctions were applied. (Note: OCR is not looking for violations in order to take enforcement action; we are restricting our analysis to whether appropriate sanctions consistent with the entity policies have been applied.)

Does the covered entity mitigate any harmful effect that is known to the covered entity of a use or disclosure of PHI by the covered entity or its business associates, in violation of its policies and procedures?

Obtain and review policies and procedures in place for consistency with the established performance criterion. Determine whether a process is in place to ensure mitigation actions are taken pursuant to the policies and procedures.

From a population of instances of non-compliance within the audit period, obtain and review documentation to determine whether mitigation plans were developed and applied pursuant to the policies and procedures. [Note: OCR is not looking for violations in order to take enforcement action; we are restricting our analysis to whether appropriate mitigation plans consistent with the entity policies have been developed and applied]

Obtain and review documentation that the policies and procedures are conveyed to the workforce.

Has the covered entity implemented policies and procedures addressing the prevention of intimidating or retaliatory actions against any individual for the exercise by the individual of any right established, or for participation in any process provided, for filing complaints against the covered entity?

Obtain and review policies and procedures in place to determine if anti-intimidation and anti-retaliatory standards exist.

Obtain and review documentation that the policies and procedures are conveyed to the workforce.

Has the covered entity required individuals to waive their right to complain to the Secretary of HHS about a covered entity or business associate not complying with these Rules, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits?

Obtain and review policies and procedures and patient/health plan member intake information to ensure that waiver is not required.

Has the covered entity implemented policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, and other requirements of the HIPAA Privacy Rule?

Obtain and review documentation that, consistent with the established performance criterion address the following:

- The policies and procedures are reasonably designed to ensure compliance for the size and type of activities performed.
- The entity changes these policies and procedures as necessary to comply with changes in the law.
- The entity documents and implements such changes promptly.
- Any corresponding material changes are made to the notice of privacy practices.

Obtain copies of policies and procedures in place in the previous calendar year and January 1, 2012, and the corresponding notices of privacy practices in effect on those dates. Determine whether material changes (e.g., for health plans, limits on use of genetic information for underwriting purposes; for health care providers, that a request for restriction must be accepted in certain situations) required by the HITECH omnibus rule are incorporated into the recent policies and procedures and are reflected in the notice of privacy practices.

Does the entity maintain all required policies and procedures, written communication, and documentation in written or electronic form?

Are such documentations retained for the required time period?

General requirements, not a part of an audit inquiry:

The Security Rule compliance practices of covered entities and business associates will be audited against the specific requirements described in the following sections. These specific requirements will be assessed based on the overarching principles set forth in the general requirements that pertain to all the security standards.

Specifically, does the covered entity or business associate:

1. Ensure confidentiality, integrity and availability of ePHI?
2. Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI?
3. Protect against reasonably anticipated uses or disclosures of ePHI that are not permitted or required by the Privacy Rule?
4. Ensure compliance with Security Rule by its workforce?

To determine which security measures the entity implements, the covered entity or business associate should take into account the following factors.

1. Its size, complexity, and capabilities.
2. Its technical infrastructure, hardware, and software security capabilities.
3. The costs of security measures.
4. The probability and criticality of potential risks to ePHI.

Use these general requirements and factors when assessing an entity's compliance with the specific requirements of the Security Rule.

Does the entity have written policies and procedures in place to prevent, detect, contain and correct security violations?

Does the entity prevent, detect, contain and correction security violations?

Obtain and review policies and procedures related to security violations. Evaluate the content relative to the specified performance criteria for countermeasures or safeguards implemented to prevent, detect, contain and correct security violations.

Obtain and review documentation demonstrating that policies and procedures have been implemented to prevent, detect, contain, correct security violations. Evaluate and determine if the process used is in accordance with related policies and procedures.

Obtain and review documentation of security violations and remediation actions. Evaluate and determine if security violations were handled in accordance with the related policies and procedures; safeguards or countermeasures to prevent violations from occurring; identify and characterize violations as they happen; limit the extent of any damages caused by violations; have corrective action plan in place to manage risk.

Does the entity have policies and procedures in place to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic protected health information (ePHI) it creates, receives, maintains, or transmits?

Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits?

Determine how the entity has implemented the requirements.

Obtain and review risk analysis policies and procedures. Evaluate and determine if written policies and procedures were developed to address the purpose and scope of the risk analysis, workforce member roles and responsibilities, management involvement in risk analysis and how frequently the risk analysis will be reviewed and updated.

Obtain and review the written risk analysis or other record(s) that documents that an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted. Evaluate and determine whether the risk analysis or other documentation contains:

- A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI
- Details of identified threats and vulnerabilities
- Assessment of current security measures
- Impact and likelihood analysis
- Risk rating

Obtain and review documentation regarding the written risk analysis or other documentation that immediately preceded the current risk analysis or other record, if any. Evaluate and determine if the risk analysis has been reviewed and updated on a periodic basis, in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event.

If there is no prior risk analysis or other record, obtain and review the two (2) most recent written updates to the risk analysis or other record, if any. If the original written risk analysis or other records have not been updated since they were originally conducted and/or drafted, obtain and review an

Does the entity have policies and procedures in place regarding a risk management process sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level?

Has the entity implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level?

Obtain and review policies and procedure related to risk management. Evaluate and determine if the documents identify how risk will be managed, what is considered an acceptable level of risk based on management approval, the frequency of reviewing ongoing risks, and identify workforce members' roles in the risk management process.

Obtain and review documentation demonstrating the security measures implemented and/or in the process of being implemented as a result of the risk analysis or assessment. Evaluate and determine whether the implemented security measures appropriately respond to the threats and vulnerabilities identified in the risk analysis according to the risk rating and that such security measures are sufficient to mitigate or remediate identified risks to an acceptable level.

Does the entity have policies and procedures in place regarding sanctions to apply to workforce members who fail to comply with the entity's security policies and procedures?

Does the entity apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures?

Obtain and review documentation of the sanction policies and procedures (which could be an aspect of a larger code of conduct). Evaluate if they contain a reasonable and appropriate process to sanction workforce members for failures to comply with the entity's security policies and procedures.

Elements to review may include but are not limited to:

- Personnel involved in the sanction process
- Required steps and time period
- Notification steps
- Reason for the sanction
- Identification of the sanctions applied to compliance failures
- Documentation of the sanction outcome

Obtain and review documentation demonstrating sanctions against workforce members. Evaluate and determine whether appropriate sanctions were applied for workforce members that failed to comply with security policies and procedures.

Does the entity have policies and procedures in place regarding the regular review of information system activity?

Does the entity regularly review records of information system activity?

Obtain and review policies and procedures related to reviewing records of information system activities. Evaluate and determine if reasonable and appropriate processes are in place to review records of information system activities, such as audit logs, access reports, and security incident tracking reports.

Elements to review may include but are not limited to:

- How often a review is performed
- How reviews are documented
- Workforce members' roles and responsibilities in the regular records of the information systems activities
- Types of activities which may require further investigation

Obtain and review documentation demonstrating the records of information system activities that were reviewed such as audit logs, access reports, and security incident tracking reports. Evaluate and determine if information system records were reviewed in a timely manner and that the review was conducted and certified by appropriate personnel.

Obtain and review documentation demonstrating the capabilities of the information system activity logs. Evaluate and determine whether key information systems have the capabilities to generate activity records; and, if so, are the capabilities turned on and records generated.

Does the entity have policies and procedures in place regarding the establishment of a security official?

Has the entity identified the security official responsible for the development and implementation of the policies and procedures required by this subpart?

Obtain and review documentation of the assigned Security Official(s) responsibilities (e.g., job description) and that a natural person has been named to act as the Security Official and/or other individuals have been assigned with other security duties. Evaluate and determine whether the organization has assigned responsibility for compliance with the Security Rule to a Security Official who oversees the development and implementation (to include monitoring and communication) of security policies and procedures and/or assigned other individuals with other security duties; and the responsibilities of the Security Official(s) have been clearly defined.

Does the entity have policies and procedures in place to ensure all members of its workforce have appropriate access to ePHI?

Does the entity ensure all members of its workforce have appropriate access to ePHI?

Obtain and review the policies and procedures that ensure all members of its workforce only have access to ePHI that is required for each workforce member to do his or her job.

Elements to review may include but are not limited to:

- That different levels of access to information systems are appropriately approved and communicated
- Ensuring that the workforce operates at privilege levels no higher than necessary to accomplish required job duties

Obtain and review documentation demonstrating access granted to workforce members and their job descriptions. Evaluate and determine that access granted to workforce members correlate with their job functions/duties.

Obtain and review documentation demonstrating that management reviews workforce members' access to information systems that contain ePHI to determine if access is appropriate. Evaluate and determine if workforce members' access to information systems that contain ePHI is certified and approved by appropriate management.

Does the entity have policies and procedures in place regarding the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed?

Does the entity authorize and/or supervise workforce member who work with ePHI or in locations where it might be accessed?

Obtain and review policies and procedures related to the authorization and/or supervision of workforce members. Evaluate the content in relation to the specified performance criteria and determine that appropriate authorization and/or supervision of workforce members who work with ePHI or in a location where it might be accessed is incorporated in the process.

Obtain and review documentation regarding how requests for information systems that contain ePHI and access to ePHI are processed. Evaluate and determine if appropriate authorization and/or supervision for granting access to information systems that contain ePHI is incorporated in the process and is in accordance with related policies and procedures.

Elements to review may include but are not limited to:

- Identification of who has the authorization and/or supervisory permission to approve access to information systems and/or locations where ePHI may be accessed
- How access requests to information systems are submitted
- How access to the information systems is granted
- How requests to access ePHI are submitted
- How access to ePHI is granted
- How authorization and/or supervisory approvals are verified
- How a workforce member's level of access to ePHI is verified

Obtain and review documentation demonstrating how access requests to locations where ePHI might be accessed are processed. Evaluate and determine if appropriate authorization for granting access to locations where ePHI might be accessed is incorporated in the process and is in accordance with related policies and procedures.

Elements to review may include but are not limited to:

- How access requests to locations are submitted
-

Does the entity have policies and procedures in place to determine that a workforce member's access to ePHI is appropriate?

Does the entity determine whether a workforce member's access to ePHI is appropriate?

Obtain and review documentation related to workforce clearance procedures. Evaluate and determine whether such procedures has been incorporated to determine whether a workforce member's access to ePHI is appropriate.

Elements to review may include but are not limited to:

- Clearing workforce members prior to authorizing access to ePHI
- Revalidation of workforce members' clearance
- Frequency of revalidating workforce members' clearance.

Obtain and review documentation demonstrating the clearance process prior to granting workforce members access to ePHI. Obtain and review documentation demonstrating approval or verification of access to ePHI (e.g., approved access request forms, electronic approval workflow, etc.). Evaluate and determine if workforce members were granted appropriate access to ePHI based on the clearance process prior to gaining access to ePHI.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place for terminating access to ePHI when employment or other arrangements with the workforce member ends?

Does the entity terminate access to ePHI when employment or other arrangements with the workforce member ends?

Obtain and review policies and procedures for terminating access to ePHI when the employment of, or other arrangement with, a workforce member's employment is terminated or job description changes to require more or less access to ePHI. Evaluate the content in relation to the specified performance criteria.

Elements to review may include but are not limited to:

- Recovery of access control devices and deactivation of information system access upon termination of employment, including voluntary termination and involuntary termination
- Termination of access by an independent contractor or other business associate, if applicable
- Appropriate changes in access levels and/or privileges pursuant to job description changes that necessitate more or less access to ePHI
- Time frames to terminate access to ePHI
- Exit interviews that include a discussion of privacy and security topics regarding ePHI

Obtain and review documentation demonstrating that workforce members' access to ePHI was terminated. Evaluate and determine whether access to ePHI was terminated in a timely manner and consistent with related policies and procedures.

Obtain and review documentation demonstrating changes in access levels for workforce members with ePHI access. Obtain and review documentation of the job duties of workforce members before and after ePHI access level was changed. Evaluate and determine whether access levels were changed appropriately and in accordance with workforce member job duties.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Does the entity have policies and procedures in place for authorizing access to ePHI that supports the applicable requirements of the Privacy Rule?

Does the entity authorize access to ePHI that supports the applicable requirements of the Privacy Rule?

Obtain and review the policies and procedures to determine that they reasonably and appropriately restrict access to only those persons and entities with a need for access. Also obtain entity's policies and procedures related to minimum necessary [45 CFR 164.502(b)] and safeguards [45 CFR 164.514(d)] to determine that the policies and procedures subject to this inquiry support an entity's compliance with the minimum necessary requirement and safeguards requirement that limit unnecessary or inappropriate access to and disclosure of protected health information.

Evaluate and determine whether the technical implementation of the access controls used by the entity support the minimum necessary policies and procedures and are consistent with the Privacy Rule safeguard policies.

If the entity is a health care clearinghouse that is part of a larger organization, does the clearinghouse have policies and procedures to protect ePHI from unauthorized access by the larger organization?

Does the clearinghouse protect ePHI from unauthorized access by the larger organization?

Obtain and review policies and procedures related to protecting ePHI held by a health care clearinghouse from unauthorized access by the larger organization. Evaluate and determine whether reasonable and appropriate administrative, physical, and technical safeguards are in place to protect against unauthorized access by the larger organization.

Does the entity have policies and procedures in place to grant access to ePHI for workforce members?

Does the entity grant access to ePHI for workforce members?

Obtain and review policies and procedures. Evaluate the content relative to the specified performance criteria for granting access, including whether authority to grant access and the process for granting access has been incorporated.

Elements to review may include but are not limited to:

- Workforce members or roles required to approve request to create information system accounts
- Procedures to create enable, modify, disable, and remove information system accounts
- Determination of what the authorization of access is based on

Obtain and review documentation associated with granting of access to ePHI (i.e., paper or electronic request). Evaluate and determine if the procedures for granting access to ePHI are in accordance with related policies and procedures.

Obtain and review documentation of newly hired workforce members' access to ePHI. Evaluate documentation to determine the granting of access to ePHI, including whether the levels of access they have to systems containing, transmitting, or processing ePHI, are appropriate.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place to authorize access and document, review, and modify a user's right of access to a workstation, transaction, program, or process?

Does the entity authorize access and document, review, and modify a user's right of access to a workstation, transaction, program, or process?

Obtain and review the policies and procedures. Evaluate their content relative to the specified performance criteria for authorizing access, and for documenting, reviewing, and modifying a user's right of access to a workstation, transaction, program, or process.

Obtain and review documentation regarding individuals whose access to information systems has been reviewed based on access authorization policies. Evaluate and determine whether individuals' access has been reviewed and recertified in a timely manner by the appropriate personnel.

Obtain and review documentation demonstrating individuals whose access to information systems has been modified based on access authorization policies. Evaluate and determine whether modification of access to information systems is acceptable and modification of individuals' access to information systems was completed and approved by appropriate personnel.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place regarding a security awareness and training program?

Does the entity provide security awareness and training to all new and existing members of its workforce?

Obtain and review policies and procedures for security awareness and training program.

Elements to review may include but are not limited to:

- How workforce members are provided the security awareness and training
- Identifies workforce members (including managers, senior executives, and as appropriate, business associates, and contractors) who will be provided with the security and awareness training
- How workforce members will be provided with security and awareness training when there is a change in the entity's information systems
- How frequently security awareness and training will be provided to all workforce members

Obtain and review documentation demonstrating the implementation of a security awareness and training program including related training materials. Evaluate and determine whether the training program is reasonable and appropriate for workforce members to carry out their functions.

Obtain and review documentation demonstrating that the security awareness and training programs are provided to the entire organization and made available to independent contractors and business associates, if appropriate.

Does the entity have policies and procedures in place regarding a process to provide periodic security reminders and updates?

Does the entity appropriately communicate security updates to all members of its workforce and, if appropriate, contractors periodically?

Obtain and review documentation demonstrating how periodic security updates are conducted.

Elements to review may include but are not limited to:

- Frequency of the periodic security updates
- Methods of communication used for security updates (i.e. emails, newsletters, posters)

Obtain and review documentation demonstrating that periodic security updates are conducted. Evaluate and determine if periodic security updates are accessible and communicated to workforce members.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place regarding a process to incorporate its procedures to guard against, detect, and report malicious software into its security awareness and training program?

Obtain and review documentation demonstrating that the procedures for guarding against, detecting, and reporting malicious software are incorporated in the security awareness and training program.

Elements to review may include but are not limited to:

- The malicious software protection mechanism that has been implemented
- Information system protection capabilities
- Workforce members' roles and responsibilities in malicious software protection procedures
- Steps to protect against malicious software
- Steps to detect malicious software
- Action(s) to be taken in response to malicious software detection

Obtain and review documentation demonstrating that procedures are in place to guard against, detect, and report malicious software. Evaluate and determine whether such procedures are in accordance with malicious software protection procedures included in the training material.

Obtain and review documentation of the workforce members who should be trained on the procedures to guard against, detect, and report malicious software.

Obtain and review documentation of the workforce members who were trained on the procedures to guard against, detect, and report malicious software. Evaluate and determine if appropriate workforce members are being trained on the procedures to guard against, detect, and report malicious software.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place to incorporate procedures for monitoring log-in attempts and reporting discrepancies into its security awareness and training program?

Obtain and review procedures (or other vehicle) for monitoring log-in and reporting discrepancies and related training material.

Elements to review may include but are not limited to:

- Workforce members' roles and responsibilities in monitoring log-in attempts and reporting discrepancies
- Identify how log-in monitoring is conducted
- How to identify an inappropriate or attempted log-in
- Action(s) to be taken in response to an inappropriate or attempted log-in

Obtain and review documentation demonstrating that procedures are in place to monitor log-in attempts and report discrepancies. Evaluate and determine whether such procedures are in accordance with the monitoring log-in attempts and reporting discrepancies procedures in the training material.

Obtain and review documentation of workforce members and role types of who should be trained on the procedures for monitoring log-in attempts and reporting discrepancies. Obtain and review documentation of the workforce members who were trained on the procedures for monitoring log-in attempts and reporting discrepancies. Evaluate and determine if appropriate workforce members are being trained on the procedures for monitoring log-in attempts and reporting discrepancies.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place to incorporate procedures for creating, changing, and safeguarding passwords into its security awareness and training program?

Obtain and review password management procedures and training (or other vehicle) for creating, changing, and safeguarding passwords.

Elements to review may include but are not limited to:

- Workforce members' roles and responsibilities in the procedures for creating, changing, and safeguarding passwords
- Identify how passwords should be created, changed, and safeguarded
- Action(s) to be taken in response to a compromised password or other authentication credential

Obtain and review documentation demonstrating that procedures for creating, changing, and safeguarding passwords are in place. Evaluate and determine whether such procedures are in accordance with the creating, changing, and safeguarding passwords procedures incorporated into the training material.

Obtain and review documentation of workforce members and role types of who should be trained on creating, changing, and safeguarding passwords. Obtain and review documentation of the workforce members who were trained on the procedures for creating, changing, and safeguarding passwords. Evaluate and determine if appropriate workforce members are being trained on the procedures for creating, changing, and safeguarding passwords.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place to address security incidents?

Obtain and review the policies and procedures related to security incidents

Elements to review may include but are not limited to:

- Identification of what specific event would be considered a security incident
- Identification of workforce members' role and responsibilities regarding security incidents
- Management involvement regarding security incidents
- Workforce members or roles to which the incident response policies and procedures are to be disseminated
- Coordination of security incidents among business associates
- Identifies what steps should be taken in response to a security incident
- The frequency to review and update current security incident policies and procedures

Obtain and review documentation demonstrating that security incident policies and procedures are implemented. Evaluate and determine whether policies and procedures are appropriate for addressing security incidents and are in accordance with related policies and procedures.

Does the entity have policies and procedures in place for identifying, responding to, reporting, and mitigating security incidents?

Does the entity identify, respond to, report, and mitigate security incidents?

Obtain and review policies and procedures related to responding and reporting security incidents. Evaluate and determine if incident response procedures are in place.

Elements to review may include but are not limited to:

- A methodology for defining security incidents based on levels of criticality
- Provisions for reporting and responding to all types of known and suspicious security incidents based on criticality levels of such incidents
- The roles and responsibilities of workforce members including the entity's security incident response team

Obtain and review documentation of responding to, reporting, and mitigating security incidents. Evaluate and determine if security incident response, reporting, and mitigation procedures are followed by workforce members; are conducted in a timely manner; and their outcomes are properly documented and communicated to the appropriate workforce members.

Does the entity have policies and procedures in place that include a formal contingency plan for responding to an emergency or other occurrences that damages systems that contain ePHI?

Does the entity have a contingency plan for responding to an emergency or other occurrences that damages systems that contain ePHI?

Obtain and review policies and procedures related to a formal contingency plan.

Elements to review may include but are not limited to:

- Identification of workforce members' roles and responsibilities in the contingency process
- Workforce members or roles to which the contingency policies and procedures are to be disseminated
- Management involvement in contingency plans
- Coordination of contingency processes among business associates
- Identification of what steps should be taken in a contingency plan
- The frequency to review and update current contingency policies and procedures
- How frequently the contingency plan is tested

Obtain and review documentation demonstrating that a contingency plan is implemented. Evaluate and determine that the response to an emergency or other occurrence that damages systems that contain ePHI include appropriate capabilities to recover access to ePHI.

Does the entity have policies and procedures in place to create and maintain retrievable exact copies of ePHI?

Does the entity create and maintain retrievable exact copies of ePHI?

Obtain and review policies and procedures related to data back-up plans. Evaluate and determine whether data back-up procedures exist that establish strategies for creating and maintaining retrievable exact copies of ePHI should the entity experience an emergency or other occurrence.

Elements to review may include but are not limited to:

- How frequently data backups will be conducted
- The type of data that will be backed up
- How data will be backed up, including the use of encryption and encryption key management, if applicable
- The backup data mechanism/solution
- How backup data will be secured
- Physical location of backup media
- Workforce members' roles and responsibilities in the data backup process
- How frequently data backups will be reviewed or assessed for verification of media reliability and data integrity

Obtain and review documentation demonstrating how data is backed up. Evaluate and determine whether the data backup process creates exact copies of ePHI.

Obtain and review documentation demonstrating data backup and restoration tests. Evaluate and determine if test procedures are in accordance with data backup plans and/or procedures; that test results are properly documented; that test results are reviewed and certified by appropriate management; and, if necessary, that corrective actions have been taken.

Does the entity have policies and procedures in place to restore any lost data?

Does the entity restore any lost data?

Obtain and review documentation related to a disaster recovery plan. Review and determine if appropriate procedures for restoring any loss of data has been incorporated into the disaster recovery plan.

Obtain and review procedures for restoring lost data. Evaluate if the procedures include all important sources of data.

Elements to review may include but are not limited to:

- Workforce members' roles and responsibilities in the process of restoring lost data
- Determination of what data will be restored
- Step-by-step process of how data will be restored
- Identify occurring events (e.g., disruption, compromise, failure) that require data restoration
- Timeframe of data restoration
- How frequently data restorations will be tested or assessed for verification of media reliability and data integrity

Obtain and review documentation of data restore tests and test results. Evaluate and determine if test procedures are in accordance with data restore plans and/or procedures; that test results are properly documented; that test results are reviewed and certified by appropriate management; and, if necessary, corrective actions have been taken.

Does the entity have policies and procedures in place to enable the continuity of critical business processes for the protection of ePHI while operating in emergency mode?

Does the entity enable the continuity of critical business processes for the protection of ePHI while operating in emergency mode?

Obtain and review procedures related to an emergency mode operation plan. Evaluate and determine whether procedures exist to enable continuation of critical business processes for the protection of the security of ePHI while operating in emergency mode.

Obtain and review documentation demonstrating the continuation of critical business processes for the protection of the security of ePHI while operating in emergency mode. Evaluate and determine if the process is appropriate and/or in accordance with related policies and procedures.

Does the entity have policies and procedures for periodic testing and revisions of its contingency plans?

Does the entity periodically test and revise its contingency plans?

Obtain and review policies and procedures related to periodic testing and revision of contingency plans.

Elements to review may include but are not limited to:

- Methods used to test the plan (component, system, or comprehensive)
- Workforce members' roles and responsibilities in coordination of the test
- How frequently tests will be conducted
- How frequently contingency plans will be revised
- Notification procedures

Obtain and review documentation demonstrating the revision of contingency plans. Based on related procedures, evaluate and determine if the contingency plans have been approved, reviewed, and updated on a periodic basis.

Obtain and review documentation of contingency plan tests and related results. Evaluate and determine if the results of each contingency plan test indicate that tests have been conducted in a timely manner; involved the appropriate workforce members; has been documented; and, if necessary, that corrective actions were taken as result of the contingency plan test.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place to assess the relative criticality of specific applications and data in support of other contingency plan components?

Does the entity assess the relative criticality of specific application and data in support of other contingency plan components?

Obtain and review documentation of critical ePHI applications and their assigned criticality levels. Evaluate and determine if application criticality levels were assessed and categorized based on importance to business needs or patient care, in order to prioritize for data backup, disaster recovery, and emergency operations plans.

Obtain and review documentation of the procedures regarding how ePHI applications (data applications that store, maintain or transmit ePHI) are identified. Evaluate and determine whether all critical ePHI applications are identified.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place to perform periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes or newly recognized risk affecting the security of ePHI?

Does the entity perform periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes or newly recognized risk affecting the security of ePHI?

Obtain and review documentation of policies and procedures related to technical and nontechnical evaluation. Determine if such policies and procedures identifies how the evaluation of findings, remediation options and recommendations, and remediation decisions are documented; specifies that evaluations will be repeated on a periodic basis and/or when environmental and operations changes are made and/or newly recognized risk affects the security of ePHI; and identifies the frequency of when to evaluate and update the current policy and procedures.

Elements to review may include but are not limited to:

- Workforce members' roles and responsibilities in the technical and nontechnical evaluation
- Management involvement in the process and approval of technical and nontechnical evaluation
- Coordination of technical and nontechnical evaluation among departments
- Specification of how technical and nontechnical evaluation will be conducted
- How technical and nontechnical evaluation findings will be addressed

Obtain and review documentation demonstrating periodic technical and non-technical evaluations. Evaluate and determine if the such evaluation appropriately evaluates ePHI security measures; addresses evaluation findings associated with noncompliant security measures; identifies and measures risks associated with noncompliant security measures; and that evaluation findings are reviewed and certified by appropriate management.

Obtain and review documentation of procedures for technology change control/management and documentation of major technology changes which affected the security of ePHI. Obtain and review documentation of plans related to risk management or mitigation efforts in response to evaluations conducted due to a major technology change which affected the security of ePHI. Evaluate and

Does the entity have policies and procedures in place to obtain satisfactory assurances from its business associates (or business associate subcontractors if the entity is a business associate) and to review the satisfactory assurances to ensure the applicable requirements at § 164.314(a) are included in the business associate contract or other arrangement?

Obtain and review documentation identifying all business associates. Obtain and review the business associate agreements and/or contracts. Using sampling methodology, evaluate and determine whether business associate agreements/contracts exist and that security requirements are in place to address the confidentiality, integrity, and availability of ePHI.

[This inquiry is for BAs only]

Based upon the selection methodologies from the above paragraph, determine whether the business associate contract identifies if it utilizes any subcontractors. If so, review the business associate agreement to examine if (i) Omnibus provisions are required and (ii) all subcontractors who create, receive, maintain, or transmit electronic protected health information on a business associate's behalf maintain business associate agreements equal to or greater than the business associate agreement with the original covered entity.

[This inquiry is for BAs only]

Does the entity have policies and procedures in place to obtain satisfactory assurances from its business associates (or business associate subcontractors if entity is a business associate) and to review the satisfactory assurances to ensure the applicable requirements at § 164.314(a) is included in the written contract or other arrangement?

Obtain and review documentation of all business associates. Obtain and review the written agreements or other arrangements (i.e., a Memorandum of Understanding if the covered entity and business associate are government agencies). Using sampling methodology, evaluate and determine whether a written contract or other arrangement exist and that security requirements are in place to address the confidentiality, integrity, and availability of ePHI. (NOTE: Business associate contracts should have been updated in 2013)

[This inquiry is for BAs only]

Based upon the selection methodologies from the above paragraph, evaluate and determine whether the written contract or other arrangement identifies if there are any subcontractors. If so, review the written contract or other arrangement to examine if (i) Omnibus provisions are required and (ii) all subcontractors who create, receive, maintain, or transmit electronic protected health information on a business associate's behalf maintain business associate agreements equal or greater than the business associate agreement with the original covered entity.

[This inquiry is for BAs only]

Does the entity have policies and procedures in place regarding access to and use of facilities and equipment that house ePHI?

Does the entity limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed?

Obtain and review policies and procedures regarding facility access control. Evaluate the content in relation to the relevant specified performance criteria regarding physical access to electronic information systems and use of facilities and equipment that house ePHI.

Evaluate and determine if policies and procedures identify the countermeasures implemented to control physical access and to detect, deter, and/or prevent unauthorized access and unlimited access to electronic information systems and facilities where systems are housed.

Elements to review may include but are not limited to:

- Workforce members' roles and responsibilities in facility access control procedures
- Management involvement in the facility's access controls procedures
- The process of how authorization credentials for facility access are issued
- The process of removing workforce members' authorization credentials for physical access when such access it is no longer required
- Identification of how visitors' access is monitored
- Methods for controlling and managing physical access devices
- Facilities and areas that have physical access control implemented to safeguard ePHI

Obtain and review documentation of workforce members with authorized physical access to electronic information systems and the facility or facilities in which they are housed. Evaluate and determine if authorized workforce members are listed in areas where electronic information system resides; listed authorized members have been approved by appropriate management; list of authorized workforce members are reviewed on a continuous basis; and removed when access is no longer required.

Obtain and review documentation of procedures for granting individuals access to entity facility or facilities where electronic information systems are housed. Evaluate and determine if physical access authorization is enforced at entry/exit points of the facility; individual access authorization is verified

Does the entity have policies and procedures in place that allow facility access for the restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency?

Does the entity allow facility access for the restoration of lost data under the Disaster Recover Plan and Emergency Mode Operation Plan in the event of an emergency?

Obtain and review contingency operations procedures. Evaluate the content in relation to the specified performance criteria that allow facility access for the restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of all types of potential disasters.

Elements to review may include but are not limited to:

- Identification of who will need access to ePHI in the event of a disaster
- Backup up plan for access to the facility and/or ePHI
- Workforce member roles and responsibilities from implementing the contingency plan for accessing ePHI in each department, unit, etc.
- Procedures for accessing restored data at the alternate processing, storage, and work site
- Procedures for the testing contingency operations

Obtain and review documentation demonstrating contingency operation procedures currently implemented. Evaluate and determine if processes are in accordance with related policies and procedures.

Obtain and review documentation demonstrating that contingency operation procedures are tested. Evaluate and determine if testing is conducted on a periodic basis and testing results are documented, including a plan of corrective actions, if necessary.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to

Does the entity have policies and procedures in place to safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft?

Does the entity safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft?

Obtain and review policies and procedures related to the facility security plan. Evaluate the content in relation to the specified performance criteria for safeguarding the facility and equipment therein from unauthorized physical access, tampering, and theft.

Elements to review may include but are not limited to:

- Identification of the physical security measures in place to provide physical security protection for facilities and equipment
- Workforce members' roles and responsibilities regarding the facility security plan
- Inventory of the entity's facilities that house equipment that create, maintain, receive, and transmit ePHI

Obtain and review documentation demonstrating that facility security plan procedures are implemented to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Evaluate and determine if implementation of the facility security plan is being followed appropriately and is in accordance with related policies and procedures.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place for controlling a person's access to facilities based on their role or function including visitor control and control of access to software programs for testing and revision?

Does the entity control a person's access to facilities based on their role or function including visitor control and control of access to software programs for testing and revision?

Obtain and review procedures related to access control and validation. Evaluate the content in relation to the specified performance criteria for controlling a person's facility access including workforce members, contractors, visitors and probationary employees.

Elements to review may include but are not limited to:

- Methods for controlling and validating an employee's access to the facility
- Workforce members' roles and responsibilities in the access control and validation process
- Frequency of reviewing lists of individuals with physical access to sensitive facilities
- Methods to control visitor's physical access to facilities

Obtain and review documentation demonstrating the control of visitor's physical access to facilities. Evaluate and determine if physical controls identify visitors attempting to access facility, prevent unauthorized visitors, and grant access to authorized visitors.

Obtain and review documentation demonstrating control of access to software program for modification and revision. Evaluate and determine if authorized individuals, roles, or job functions are identified and validated before gaining access to software program and is in accordance with applicable procedures.

Obtain and review documentation demonstrating facility and software access control and validation procedures are implemented.

Evaluate and determine if safeguards implemented overall controls access to facility physical environment, by validating individuals roles or function before granting physical access to facility or software programs; deter and prevent unauthorized access to the facility or software in accordance with applicable policies and procedures.

Does the entity have policies and procedures in place to document repairs and modifications to the physical components of a facility which are related to security?

Does the entity document repairs and modifications to the physical components of a facility which are related to security?

Obtain and review such policies and procedures related to maintaining maintenance records. Evaluate the content in relation to the specified performance criteria for documenting repairs and modifications to the physical components of a facility related to security.

Elements to review but are not limited to:

- Workforce members' roles and responsibilities in repairs and modification to the physical components
- Record keeping process of repairs and modification to the physical components
- Specification of when repairs or modification of physical security components are required
- Authorization process of repairs or modification of physical security components

Obtain and review documentation demonstrating records of repairs and modifications to physical security components. Evaluate and determine if records of repairs and modifications are being tracked and reviewed on periodic basis by authorized personnel.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place that specifies the proper functions to be performed and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI?

Does the entity specify the proper functions to be performed and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI?

Obtain and review such policies and procedures related to workstation use. Evaluate the content in relation to the specified performance criteria for the proper functions to be performed by electronic computing devices.

Elements to review may include but are not limited to:

- Process to identify workstations by type and location
- Specify the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI (e.g. to prevent or preclude unauthorized access to an unattended workstation, limit the ability of unauthorized persons to view sensitive information as needed)
- Procedures related to the proper use and performance of workstations
- Workforce members roles and responsibilities in the workstation use process

Obtain and review an inventory of the locations and types of workstations. Evaluate and determine if an inventory exists of workstation; when the inventory was last updated; and whether there is a documented process for updating the inventory. If available, review the inventory to see if it includes the types of ePHI data elements contained on the systems included in the inventory.

Obtain documentation demonstrating workstation classification. Evaluate and determine if each workstation is classified based on the specific workstation's capabilities, connection, and allowable activities.

Obtain and review documentation demonstrating workstation use policies and procedures implemented. Evaluate if such implementation is in accordance with related policies and procedures.

Does the entity have policies and procedures that document how workstations are physically restricted to limit access to only authorized personnel?

Does the entity workstations that access electronic protected health information restricted to authorized users?

Obtain and review policies and procedures related to workstation security. Evaluate the content in relation to the specified criteria for security measures and guidance on how to implement and maintain physical security and how physical access to workstations that access ePHI is restricted to appropriate personnel.

Obtain and review documentation demonstrating workstation security policies and procedures being implemented. Evaluate and determine if implementation is appropriate and is in accordance with related policies and procedures.

Does the entity have policies and procedures in place that govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within the facility?

Does the entity govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within facility?

Obtain and review the policies and procedures related to device and media controls. Evaluate the content in relation to the specified performance criteria for the proper handling of electronic media that contain ePHI.

Elements to review may include but are not limited to:

- How are the types of hardware and electronic media that must be tracked (both entity owned and personally owned) are identified
- The process of tracking all types of hardware and electronic media that contain ePHI
- Workforce members' roles and responsibilities in the device and media control process
- Authorization process for the receipt and removal of hardware and electronic media that store ePHI
- How the release of hardware, software, and ePHI data out of entity control is managed and documented

Obtain and review documentation demonstrating the movement of hardware and electronic media containing ePHI into, out of and within the facility. Evaluate and determine if movement of hardware and electronic media is being properly tracked, documented, and approved by appropriate personnel.

Obtain documentation demonstrating the type of security controls implemented for the facility in, out, and within movements of workforce members' assigned hardware and electronic media that contain ePHI. Evaluate and determine if security controls are appropriate, properly implemented, and minimize possible vulnerabilities.

Does the entity have policies and procedures that address the disposal ePHI data, hardware or electronic media on which it is stored?

Does the entity address the disposal ePHI data, hardware or electronic media on which it is stored?

Obtain and review policies and procedures related to disposal of any electronic media that stores ePHI. Evaluate the content in relation to the specified performance criteria for the disposal of hardware, software, and ePHI.

Elements to review may include but are not limited to:

- How the disposal of ePHI and or the hardware or electronic media that stores ePHI is managed and documented
- Identification of how the sanitization process of information system media is managed and documented
- Workforce members' roles and responsibilities in the device and media disposal process
- Identification of how the disposition of previous stored ePHI and/or the hardware or electronic media is verified
- Identify the types of devices and media that store ePHI

Obtain and review documentation demonstrating how the disposal of hardware, software, and ePHI data is completed, managed, and documented. Evaluate and determine if process is being followed appropriately and is in accordance with related policies and procedures.

Obtain and review documentation demonstrating how the sanitization of electronic media is completed, managed, and documented. Evaluate and determine if process is being followed appropriately and is in accordance with related policies and procedures.

Does the entity have policies and procedures established to remove ePHI before reusing electronic media and who is responsible for the overseeing those processes?

Does the entity remove ePHI before reusing electronic media and who is responsible for the overseeing those processes?

Obtain and review procedures related to media re-usage. Evaluate the content in relation to the specified performance criteria for removing ePHI from electronic media before they are issued for reuse.

Elements to review may include but are not limited to:

- Workforce members' roles and responsibilities in the media re-use process
- How the removal of ePHI from electronic media is verified
- How ePHI will be removed from electronic media before external and internal re-use

Obtain documentation demonstrating media re-use procedures being implemented and how ePHI has been removed from electronic media. Evaluate and determine if the process used for the reuse of electronic media is appropriate; that ePHI is properly removed from electronic media prior to reuse; that ePHI that is removed is unusable, inaccessible, and indecipherable; and that removal of ePHI from electronic media has been verified prior to reuse of electronic media.

Does the entity have policies and procedures to record the movements of hardware and electronic media and any person responsible therefore?

Does the entity record the movements of hardware and electronic media and any person responsible therefore?

Obtain and review policies and procedures related to device and media accountability. Evaluate the content relative to the specified performance criteria regarding tracking the location of electronic media and hardware (including entity-owned and personally-owned electronic/mobile devices and media containing, or with access to, ePHI) and maintaining records of movements of, and individual(s) responsible for, hardware and electronic media that has access or contains ePHI.

Elements to review may include but are not limited to:

- Workforce members' roles and responsibilities in the device and media accountability process
- How records of movements of electronic media and hardware are maintained
- The processing of reviewing and certifying movements of hardware and electronic media records
- Identify the types of hardware and electronic media that will be tracked in the device and media accountability process

Obtain and review documentation demonstrating a record of movements of hardware and electronic media and person responsible therefore. Evaluate and determine if media and hardware (including entity-owned and personally owned electronic/mobile devices and media) are tracked, recorded, and certified by appropriate personnel.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place to create a retrievable, exact copy of ePHI when needed, before movement of equipment?

Does the entity create retrievable, exact copy of ePHI when needed, before movement of equipment?

Obtain and review policies and procedures related to data backup and storage procedures. Evaluate the content relative to the specified performance criteria to determine whether policies and procedures cover creating a retrievable exact copy of electronic protected health information, when needed, before movement of equipment.

Elements to review may include but are not limited to:

- Identify when ePHI data backups will be conducted
- The type of data that will be backed up
- How data will be backed up, including the use of encryption and encryption key management, if applicable
- Backup data mechanism/solution
- How backup data is secured
- Identification of how and where backup ePHI data is physically stored and secured
- Workforce members' roles and responsibilities in the data backup and storage process
- How frequently data backups are reviewed or assessed for verification of media reliability and data integrity

Obtain and review documentation demonstrating how ePHI data is backed up for equipment being moved to another location. Evaluate and determine if ePHI data backup process is appropriate and is in accordance with the entity's data backup plan and/or procedures.

Obtain and review documentation demonstrating how ePHI data backups for moved equipment are stored. Evaluate and determine if the backup data is stored in a location with minimum vulnerabilities and appropriate safeguards and that the confidentiality, integrity, and availability of the ePHI data is protected from security threats.

Obtain and review documentation demonstrating the restoration of ePHI data backups for moved equipment. Evaluate and determine if the procedure is in accordance with backup plans and/or

Has the entity implemented technical policies and procedure for the electronic information systems that maintain ePHI to allow access only to authorized users?

Does the entity only allow access to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) to electronic information systems that maintain electronic protected health information?

Obtain and review policies and procedures related to access control. Evaluate the content relative to the specified performance criteria to determine if ePHI is only accessible to authorized persons or software programs.

Elements to review may include but are not limited to:

- Identification of the capabilities of electronic information system access controls (i.e., read-only, modify, full access)
- Identification of the type of access controls implemented for the electronic information systems
- Identification of how system and generic IDs/accounts are implemented, managed and controlled by technical access controls
- Workforce members' roles and responsibilities regarding the capabilities to add, modify, or delete user access
- The frequency of review and verification of user access to electronic information systems that maintain ePHI
- The frequency of review and verification of software program access to electronic information systems that maintain ePHI
- How is removed upon termination or modified upon change of position

Obtain and review documentation demonstrating the implementation of access controls for electronic information systems that maintain ePHI. Evaluate and determine if the electronic information systems have the capacity to enable access controls; if access controls can be enabled, are the enabled access controls configured in accordance with the access control policies and procedures; and how are the electronic information systems' technical access capabilities defined (i.e., read-only, modify, full-access).

Obtain and review documentation demonstrating a list of new workforce members from the electronic

Does the entity have polices and procedures regarding the assignment of unique user IDs to track user identity?

Does the entity assign unique user IDs to track user identity?

Obtain and review policies and procedures regarding the assignment of unique user IDs. Evaluate the content of the policies and procedures in relation to the specified performance criteria to determine how user IDs are to be established and assigned.

Obtain and review documentation demonstrating the assignment, creation, and use of unique user IDs in electronic information systems for user. Evaluate and determine if users are assigned a unique ID in accordance with the entity's policies and procedures for attributing new user IDs.

Does the entity have policies and procedures in place to provide access to ePHI during an emergency?

Does the entity provide access to ePHI during an emergency?

Obtain and review procedures related to emergency access. Evaluate the content in relation to the specified criteria to determine if an emergency access procedure is in place for obtaining necessary ePHI during an emergency.

Elements to review may include but are not limited to:

- Procedures in place to provide necessary access to ePHI during an emergency
- How access to initiate emergency access to ePHI is limited to appropriate personnel
- How access to ePHI is normalized once an emergency situation has passed
- Workforce members roles and responsibilities in the emergency access procedures

Obtain and review documentation demonstrating a list of workforce members with authority to initiate the emergency access procedures. Evaluate and determine if list of workforce members correlates with workforce members listed in the emergency access procedures. Obtain and review documentation demonstrating technical systems limiting emergency access initiation. Evaluate and determine whether technical systems have the capability to limit emergency access initiation to authorized workforce members only.

Does the entity have policies and procedures in place to automatically terminates an electronic session after a predetermined time of inactivity?

Does the entity automatically terminates an electronic session after a predetermined time of inactivity?

Obtain and review policies and procedures regarding automatic logoff. Evaluate the content in relation to the specified criteria to determine whether it specifies that an electronic session is terminated after a predetermined time of inactivity.

Obtain and review documentation (e.g., screenshots, system settings, etc.) demonstrating the implementation of automatic logoff. Evaluate and determine if automatic logoff settings are implemented in accordance with related policies and procedures.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review documentation of why it was determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate the documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place to encrypt and decrypt ePHI including processes regarding the use and management of the confidential process or key used to encrypt and decrypt ePHI?

Does the entity encrypt and decrypt ePHI including processes regarding the use and management of the confidential process or key used to encrypt and decrypt ePHI?

Obtain and review the policies and procedures regarding the encryption and decryption of ePHI. Evaluate the content relative to the specified criteria to determine that the implementation and use of encryption appropriately protects ePHI.

Elements to review may include but are not limited to:

- Type(s) and documentation of encryption technology used for devices and media that contain or have access to ePHI
- How the confidential processes or keys used for encryption and decryption are managed and protected
- How access to modify or create keys is restricted to appropriate personnel

Obtain and review documentation demonstrating ePHI being encrypted and decrypted. Evaluate and determine if ePHI is encrypted and decrypted in accordance with related policies and procedures.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place to implement hardware, software and/or procedural mechanisms to record and examine activity in information systems that contain or use ePHI?

Does the entity have hardware, software and/or procedural mechanism to record and examine activity in information systems that contain or use ePHI?

Obtain and review documentation relative to audit controls. Evaluate whether risk-based audit controls have been implemented over all electronic information systems that contain or use ePHI.

Elements to review may include but are not limited to:

- Identification of the risk-based audit controls over all information systems that contain or use ePHI
- How are systems and applications evaluated to determine if auditing controls should be implemented
- Identification of what applications and systems will be audited
- Procedures on how systems will be audited

Obtain and review documentation demonstrating the implementation of hardware, software and/or procedural mechanisms to record and examine activity. Evaluate and determine whether information systems that contain or use ePHI activities are being recorded and examined; activities being recorded and examined appropriately and in accordance with related policies and procedures.

Does the entity have policies and procedures in place to protect ePHI from improper alteration or destruction?

Does the entity protect ePHI from improper alteration or destruction?

Obtain and review policies and procedures regarding the implementation of integrity controls to protect ePHI. Evaluate if the implemented integrity controls appropriately protect the entity's ePHI from improper alteration or destruction.

Elements to review may include but are not limited to:

- What processes are in place to protect ePHI from improper alteration or destruction
- How processes protect ePHI from improper alteration or destruction
- How processes detect improper alteration or destruction of ePHI
- What actions are taken if improper alteration or destruction of ePHI is detected

Obtain and review documentation demonstrating processes in place to protect ePHI from improper alteration or destruction. Evaluate and determine whether implementation of process is in accordance with related policies and procedures.

Obtain and review documentation demonstrating processes protecting ePHI from improper alteration or destruction. Evaluate and determine whether ePHI is properly protected from alteration or destruction; processes in place to protect ePHI correlates with safeguards identify in integrity control policies and procedures.

Does the entity have policies and procedures in place regarding the implementation of electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner?

Does the entity have electronic mechanism to corroborate that ePHI has not been altered or destroyed in an unauthorized manner?

Obtain and review policies and procedures for authenticating ePHI. Evaluate the content relative to the specified criteria to determine that electronic mechanisms are in place to authenticate ePHI.

Elements to review include but are not limited to:

- How to detect if ePHI has not been altered or destroyed
- How to detect if ePHI has been altered or destroyed in an unauthorized manner.

Obtain and review documentation demonstrating that electronic mechanisms are implemented to authenticate ePHI. Evaluate the implemented mechanisms to determine that the implemented mechanisms would appropriately corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place to verify that a person or entity seeking access to ePHI is the one claimed?

Does the entity verify that a person or entity seeking access to ePHI is the one claimed?

Obtain and review policies and procedures regarding person or entity authentication. Evaluate if systems and applications requiring authentication have been identified and whether authentication procedures have been implemented for the systems and applications that require authentication.

Elements to review may include but are not limited to:

- The authentication procedures for all systems and applications that access ePHI.
- Procedures to evaluate information systems and application authentication methods.
- The authentication process for verifying identity of a real person or an automated process or entity.

Obtain and review documentation demonstrating the implementation of authentication procedures for persons or entities seeking access to ePHI. Evaluate and determine whether the implemented authentication procedures are sufficient to verify that the persons or entity seeking access to ePHI is the one claimed.

Does the entity have policies and procedures in place to implement technical security controls to guard against unauthorized access to ePHI transmitted over electronic communications networks?

Does the entity have security controls to guard against unauthorized access to ePHI transmitted over electronic communications networks?

Obtain and review policies and procedures related to transmission security controls. Evaluate content relative to the specified criteria to determine that the technical security controls implemented guards against unauthorized access to ePHI transmitted over electronic communication networks.

Elements to review may include but are not limited to:

- Identify the various methods, devices, and networks used to electronically transmit ePHI
- The procedures to evaluate and select appropriate technical controls to secure ePHI transmitted across all of its devices and networks
- Identify the technical security controls implemented to guard against unauthorized access to ePHI transmitted over electronic communication networks

Obtain and review documentation demonstrating the implementation of technical security measures to protect electronic transmissions of ePHI. Evaluate the content in relation to the specified criteria to determine that the implemented technical security measures are sufficient to guard against unauthorized access to the electronically transmitted ePHI.

Does the entity have policies and procedures in place to implement security measures to ensure that electronically transmitted ePHI cannot be improperly modified without detection until disposed of.

Obtain and review policies and procedures related to transmission security measures. Evaluate content relative to the specified criteria to determine that the security measures are implemented to ensure that electronically transmitted ePHI cannot be improperly modified without detection.

Elements to review may include but are not limited to:

- The security measures in place to ensure that electronically transmitted ePHI has not been improperly modified without detection
- How to detect if transmitted ePHI has been improperly modified

Obtain and review documentation demonstrating the implementation of security measures to protect electronic transmissions of ePHI. Evaluate the content to determine if the implemented security measures ensure that electronically transmitted PHI cannot be improperly modified without detection.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place to implement an encryption mechanism to encrypt ePHI whenever deemed appropriate?

Does the entity have encryption mechanism to encrypt ePHI whenever deemed?

Obtain and review policies and procedures regarding the encryption of electronically transmitted ePHI. Evaluate the content relative to the specified criteria to determine that the implementation and use of encryption appropriately secures electronically transmitted ePHI.

Elements to review may include but are not limited to:

- Type(s) and documentation of encryption technology used to secure electronically transmitted ePHI
- How the confidential processes or keys used for encryption are managed and protected
- How access to modify or create keys is restricted to appropriate personnel
- Identify when it is appropriate to encrypt ePHI

Obtain and review documentation demonstrating the encrypted mechanism is implemented to encrypt ePHI. Evaluate and determine whether encrypted mechanism has the capability to encrypt ePHI when it is deemed as appropriate.

Obtain and review documentation demonstrating that electronically transmitted ePHI is encrypted. Evaluate and determine if ePHI encrypted is appropriate and in accordance with related policies and procedures.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Does the entity have policies and procedures in place regarding its contractual arrangements with contractors or other entities to which it discloses ePHI for use on its behalf?

Elements to review may include but are not limited to:

- Does the entity use a standard business associate contract with contractors or other entities to which it discloses ePHI
- What is the approval process for deviations of standard business associate contracts

Obtain and review the entity's standard business associate contract template(s). Evaluate and determine that the entity's standard business associate contract template(s) meet the requirements of 45 CFR § 164.314(a)(2)(i), § 164.314(a)(2)(ii), or § 164.314(a)(2)(iii), as applicable.

Obtain and review documentation demonstrating the entity's approval process when deviations affecting the implementation of safeguards to protect ePHI are considered. Evaluate and determine if the entity's policies for approving deviations affecting safeguards to protect ePHI are appropriate.

Does the entity have policies and procedures in place regarding the content of its business associate contracts to ensure that its business associates will comply with applicable requirements of Subpart C of 45 CFR Part 164?

Obtain and review business associate contracts. Evaluate and determine if the business associate contracts provide that the entity's business associates shall implement appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to ePHI to prevent the use or disclosure of PHI other than as provided for by the business associate contract.

Does the entity have policies and procedures in place requiring that its business associate contracts or other arrangements require that subcontractors that create, receive, maintain or transmit ePHI on behalf of its business associates agree to comply with the applicable parts of Subpart C of 45 CFR Part 164 by entering into a business associate contract or other arrangement that complies with 45 CFR § 164.314(a)?

Obtain and review business associate contracts. Evaluate and determine if the business associate contracts require that business associate's subcontractors comply with the applicable parts of Subpart C of 45 CFR Part 164 by entering into a business associate contract or other arrangement that complies with 45 CFR § 164.314(a).

Does the entity have policies and procedures in place regarding the content of its business associate contracts to ensure that its business associates will report any security incident of which it becomes aware, including breaches of unsecured PHI, as required by 45 CFR § 164.410?

Obtain and review business associate contracts. Evaluate and determine if the business associate contracts require that business associates report any security incident of which it becomes aware, including breaches of unsecured PHI, as required by 45 CFR § 164.410.

Obtain and review documentation demonstrating that the entity's business associates have reported security incidents of which it was aware, including breaches of unsecured PHI, as required by 45 CFR § 164.410.

Does the entity have policies and procedures in place regarding other arrangements to have in place (e.g., a Memorandum of Understanding if the covered entity and business associate are government agencies) that meet the requirements of 45 CFR § 164.504(e)(3)?

Obtain and review documentation of the entity's other arrangements with business associates. Evaluate and determine if the other arrangements meet the requirements of 45 CFR § 164.504(e)(3).

Does the business associate have policies and procedures in place regarding business associate contracts or other arrangements with its subcontractors such that the requirements of 45 CFR § 164.314(a)(2)(i)-(ii) would apply to the business associate and its subcontractors in the same manner as such requirements apply to a covered entity and its business associates?

Obtain and review business associate contracts entered into with subcontractors. Evaluate and determine if the business associate contracts require that the requirements of 45 CFR § 164.314(a)(2)(i)-(ii) would apply to the business associate and its subcontractor in the same manner as such requirements apply to a covered entity and its business associates.

Does the group health plan have policies and procedures in place to ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan?

Obtain and review plan documents. Evaluate and determine that, except when the only ePHI disclosed to a plan sponsor is in accordance with 45 CFR § 164.504(f)(1)(ii) or (iii) or authorized under 45 CFR § 164.508, that the plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan.

Do the plan documents of the group health plan include language that requires the sponsor to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan?

Obtain and review plan documentation. Evaluate and determine that the plan documents of the group health plan requires the sponsor to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan.

Do the plan documents of the group health plan incorporate provisions to ensure that adequate separation required by 45 CFR § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures?

Obtain and review plan documentation. Evaluate and determine that the plan documents of the group health plan ensures adequate separation between the group health plan and the plan sponsor, including the sponsor's employees, classes of employees, or other persons who will be given access to the ePHI.

Do the plan documents of the group health plan incorporate provisions to include language that requires the sponsors to ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information?

Obtain and review plan documentation. Evaluate and determine that the plan documents of the group health plan requires that plan sponsors ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.

Do the plan documents of the group health plan incorporate provisions to include language that requires plan sponsors to report to the group health plan any security incident of which it becomes aware?

Obtain and review plan documentation. Evaluate and determine that the plan documents of the group health plan requires that plan sponsors report to the group health plan any security incident, including any breach of unsecured ePHI, of which it becomes aware.

Does the entity have policies and procedures in place to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specification or other requirements of the Security Rule?

Obtain and review documentation of the policies and procedures regarding the implementation of policies and procedures required to comply with Security Rule standards, implementation specifications or other requirements.

Does the entity have policies and procedures to maintain written policies and procedures related to the security rule and written documents of (if any) actions, activities, or assessments required of the security rule?

Obtain and review policies and procedures regarding the maintenance of policies and procedures.

Obtain and review documentation demonstrating that policies and procedures are being maintained.

Obtain and review written documentation demonstrating the entity's action, activity or assessment that is required by the Security Rule. Evaluate and determine if such implementation is in accordance with related policies and procedures.

Does the entity have policies and procedures in place regarding the retention of required documentation for six (6) years from the date of its creation or the date when it last was in effect?

Obtain and review documentation of policies and procedures for compliance with retention requirements.

Obtain and review documentation demonstrating that policies and procedures are being maintained for six (6) years from the date of its creation or the date when it last was in effect.

Obtain and review documentation demonstrating that an action, activity, or assessment is being maintained for six (6) years from the date of its creation or the date when it last was in effect. Evaluate and determine if such implementation is in accordance with related policies and procedures.

Does the entity have policies and procedures in place requiring that documentation be made available to the workforce members responsible for implementing applicable Security Rule policies and procedures?

Obtain and review documentation of policies and procedures regarding the availability of documentation.

Obtain and review documentation demonstrating that Security Rule policies and procedures are made available to the workforce members responsible for implementing the pertaining procedures. Evaluate and determine if implementation is in accordance with related policies and procedures.

Does the entity have policies and procedures in place to perform periodic reviews and updates to Security Rule policies and procedures?

Obtain and review policies and procedures regarding documentation reviews and updates.

Obtain and review documents demonstrating that policies and procedures are reviewed and updated on a periodic basis. Evaluate and determine if such implementation is in accordance with related policies and procedures.

164.414(a)

Administrative Requirements: Has the covered entity adequately implemented the required 164.530 provisions as they relate to the Breach Notification Rule? Inquire of management.

164.530(b) - Training

Obtain and review the covered entity's policies and procedures. Evaluate whether they are consistent with the requirement to provide training pertaining to the Breach Notification Rule.

Has the covered entity trained its workforce on the applicable provisions?

- Obtain and review the content of covered entity's training materials
- Obtain and review evidence that all workforce members received the training, e.g., training sign in sheets.

164.530(d) - Complaints to the covered entity

Obtain and review the covered entity's policies and procedures. Evaluate whether they are consistent with the requirement to provide a process for individuals to complain about the covered entity's compliance with the Breach Notification Rule.

Does the covered entity have a process in place for individuals to complain about its compliance with the Breach Notification Rule?

Has the covered entity received any such complaints? If yes, obtain and review a list of complaints received in the specified period and the disposition of such complaints, including documentation of actions taken by the covered entity or business associate to investigate and resolve the potential breach. Use sampling methodologies to select complaints to be reviewed and verify that actions taken were consistent with the requirements of the Breach Notification Rule.

164.530(e) – Sanctions

Obtain and review the covered entity's policies and procedures. Evaluate whether they are consistent with the requirement to sanction a covered entity's workforce members.

Has the covered entity sanctioned any workforce members for failing to comply with its policies and procedures as they relate to the Breach Notification Rule? If yes, obtain and review a complete list of sanctions, including the type of sanction applied and the type of action that led to the sanction and any other relevant information. Use sampling methodologies to select sanctions to be reviewed and verify that actions taken were consistent with the requirements of the Breach Notification Rule.

164.530(g) – Refraining from Retaliatory Acts

Does the covered entity have appropriate policies and procedures in place to prohibit retaliation against any individual for exercising a right or participating in a process (e.g., assisting in an investigation by HHS or other appropriate authority or for filing a complaint) or for opposing an act or practice that the person believes in good faith violates the Breach Notification Rule? Obtain and review such policies and procedures.

164.530(h) – Waiver of Rights

Does the covered entity have appropriate policies and procedures in place to prohibit it from requiring an individual to waive any right under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits? Obtain and review such policies and procedures. If patient or health plan member intake forms are used, obtain and review to confirm that such a requirement is not contained within them.

164.530(i) – Policies and Procedures

Does the covered entity have policies and procedures that are consistent with the requirements of the Breach Notification Rule?

- Obtain and review the covered entity's policies and procedure for evaluating the appropriate action under the Breach Notification Rule when there is an impermissible use or disclosure of PHI.
- Obtain and review the covered entity's policies and procedures for providing notifications to individuals, the media (if applicable), and the Secretary.
- Obtain and review the covered entity's policies and procedures for requiring business associates to report an impermissible use or disclosure of PHI to the covered entity and the covered entity's process for handling such reports.

164.530(j) - Documentation

Does the covered entity have policies and procedures for maintaining documentation consistent with the requirements at §164.530(j)?

- Obtain and review documentation that the covered entity maintains its policies and procedures, in written or electronic form, until 6 years after the later of the date of their creation or the last effective date.
 - Obtain and review documentation that the covered entity maintains all other documentation required by 164.530(j)(1) until 6 years after the later of the date of their creation or the last effective date.
-

§164.402 Definitions: Breach - Risk Assessment

Does the covered entity have policies and procedures for determining whether an impermissible use or disclosure requires notifications under the Breach Notification Rule?

Does the covered entity have a process for conducting a breach risk assessment when an impermissible use or disclosure of PHI is discovered, to determine whether there is a low probability that PHI has been compromised?

If not, does the covered entity have a policy and procedure that requires notification without conducting a risk assessment for all or specific types of incidents that result in impermissible uses or disclosures of PHI?

Obtain and review policies and procedures regarding the process for determining whether notifications must be provided when there is an impermissible acquisition, access, use, or disclosure of PHI.

If the entity does not have a policy and procedure that treats all potential breaches as requiring notifications without conducting a risk assessment, review the covered entity's risk assessment policies and procedures. Evaluate whether they require the covered entity to consider at least the following four factors:

- (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- (ii) The unauthorized person who used the PHI or to whom the disclosure was made
- (iii) Whether the PHI was actually acquired or viewed
- (iv) The extent to which the risk to the PHI has been mitigated.

§164.402 - Definitions: Breach Exceptions - Unsecured PHI

Did the covered entity or business associate determine that an acquisition, access, use or disclosure of protected health information in violation of the Privacy Rule not require notifications under §§164.404-164.410 within the specified period?

- If yes, did the covered entity or business associate determine that one of the regulatory exceptions to the definition of breach at §164.402(1) apply? If yes, obtain documentation of such determination. Use sampling methodologies to select and review documentation that such were completed in accordance with §164.402.

- If yes, did the covered entity or business associate determine that the breach did not require notification, under §§164.404-410, because the PHI was not unsecured PHI, i.e., it was rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in the applicable guidance? If yes, obtain and review documentation. Use sampling methodologies to select and review documentation that such were completed in accordance with §164.402.

§164.404(a)(1)

Notice to Individuals

Does the covered entity have policies and procedures for notifying individuals of a breach of their protected health information.

Obtain and review a list of breaches, if any, in the specified period involving 500 or more individuals. Obtain and review documentation of notifications provided to the affected individuals. Determine whether notifications were provided to individuals consistent with the requirements in §164.404(a)(1).

§164.404(b)

Timeliness of Notifications

Were individuals notified of breaches within the required time period? Inquire of management.

Obtain and review the policies and procedures for notifying individuals of breaches and determine whether such policies and procedures are consistent with §164.404, including providing notification without unreasonable delay and in no case later than within 60 days of discovery of a breach.

Obtain and review a list of breaches, if any, in the specified period and documentation indicating the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for delay in notification to determine whether all individuals were notified consistent with §164.404(a), (b).

§164.404(c)(1)

Content of Notification

Does the covered entity have policies and procedures for providing individuals with notifications that meet the content requirements of §164.404(c)? Inquire of management; obtain and review policies and procedures. Evaluate if the specifications at §164.404(c) are met.

Inquire of management whether the covered entity has used a standard template or form letter for notification to individuals for all breaches or for specific types of breaches. If the covered entity has used a standard template or form letter for breach notification, obtain and review the document. Evaluate whether it includes this section's required elements.

Obtain and review a list of breaches, if any, in the specified period and documentation of written notices sent to affected individuals for each breach. Use sampling methodologies to select notifications sent to individuals to be reviewed and verify that the notices include the elements required by §164.404(c).

§164.404(d)

Methods of Notification

Does the covered entity have policies and procedures for notifying an individual, an individual's next of kin, or a personal representative of a breach? Inquire of management.

Obtain and review the covered entity's policies and procedures for notifying individuals, next of kin, or personal representatives of a breach to determine whether they are consistent with §164.404(d), including the following:

- Do the policies and procedures provide that notice will be provided by first-class mail unless the individual has agreed to receive an electronic notice?
If there is a process for individuals to agree to receive electronic notice, is there also a process to address circumstances where an individual withdraws such agreement?

- Do the policies and procedures provide that the covered entity will send the notification to the next of kin or personal representative where the covered entity has knowledge that the individual is deceased and has the address of the next of kin or personal representative?

- Do the policies and procedures address the provision of substitute notice consistent with §164.404(d)(2), including:
 - o Alternative means for providing notification to individuals if there is insufficient or out-of-date contact information for fewer than 10 individuals
 - o If insufficient or out-of-date contact information for 10 or more individuals
 - Posting a conspicuous notice on the home page of the covered entity's web site or publishing conspicuous notices in major print or broadcast media in the geographic area(s) where the affected individuals likely reside
 - Establishing a toll-free phone number that remains active for at least 90 days.

Did the covered entity determine that there were any breaches within the specified period that required substitute notice? Obtain and review documentation of substitute notices:

1. If insufficient or out-of-date contact information for fewer than 10 individuals, documentation of notice provided by alternative means, such as a log of telephone call
2. If insufficient or out-of-date contact information for 10 or more individuals, documentation of a

§164.406(a)

Notification to the Media

Does the covered entity have policies and procedures for notifying media outlets of breaches affecting more than 500 residents of a State or jurisdiction? Obtain and review policies and procedures. Evaluate whether the specifications at §164.406 are met.

Obtain and review a list of breaches, if any, in the specified period affecting more than 500 residents of a State or jurisdiction. Obtain and review documentation to verify that the media notifications included the elements required by §164.406.

§164.408

Notification to the Secretary

Does the covered entity have policies and procedures for notifying the Secretary of breaches involving 500 or more individuals? Does the covered entity have policies and procedures for notifying the Secretary of breaches involving less than 500 individuals? Obtain and review policies and procedures. Evaluate whether the specifications at §164.408 are met.

Obtain and review a list of breaches, if any, in the specified period involving 500 or more individuals. Obtain and review documentation of notifications provided to the Secretary. Determine whether contemporaneous notifications were provided to the Secretary consistent with the requirement in §164.408. Use sampling methodologies to select notifications to be reviewed and verify that the notices include the elements required by §164.408.

Obtain and review a list of breaches, if any, in the specified period involving fewer than 500 individuals. Obtain and review documentation of notifications provided to the Secretary . Evaluate whether the notifications were provided to the Secretary within 60 calendar days of the end of the calendar year in which the breach was discovered, consistent with the requirement in §164.408. Use sampling methodologies to select notifications to be reviewed and verify that the notices include the elements required by §164.408.

§ 164.410

Notification by a Business Associate

Did the business associate or subcontractor determine that there were any breaches of unsecured PHI within the specified period?

If yes, obtain copies of the notification(s) sent by the business associate (or subcontractor) to the covered entity (or business associate for breaches by subcontractors). Evaluate whether the business associate or subcontractor sent the notifications consistent with the requirements at §164.410. Use sampling methodologies to select notifications to be reviewed and verify that the notices include the elements required by §164.410.

§164.412

Law Enforcement Delay

Does the covered entity or business associate have policies and procedures regarding how the covered entity or business associate would respond to a law enforcement statement that a notice or posting would impede a criminal investigation or damage national security?

Has the covered entity or business associate delayed notification of a breach of unsecured PHI pursuant to such a law enforcement statement?

If yes, obtain and review documentation of any such law enforcement statement. Evaluate whether the covered entity or business associate acted in accordance with §164.412. Use sampling methodologies to select notifications to be reviewed and verify that the notices include the elements required by §164.412.

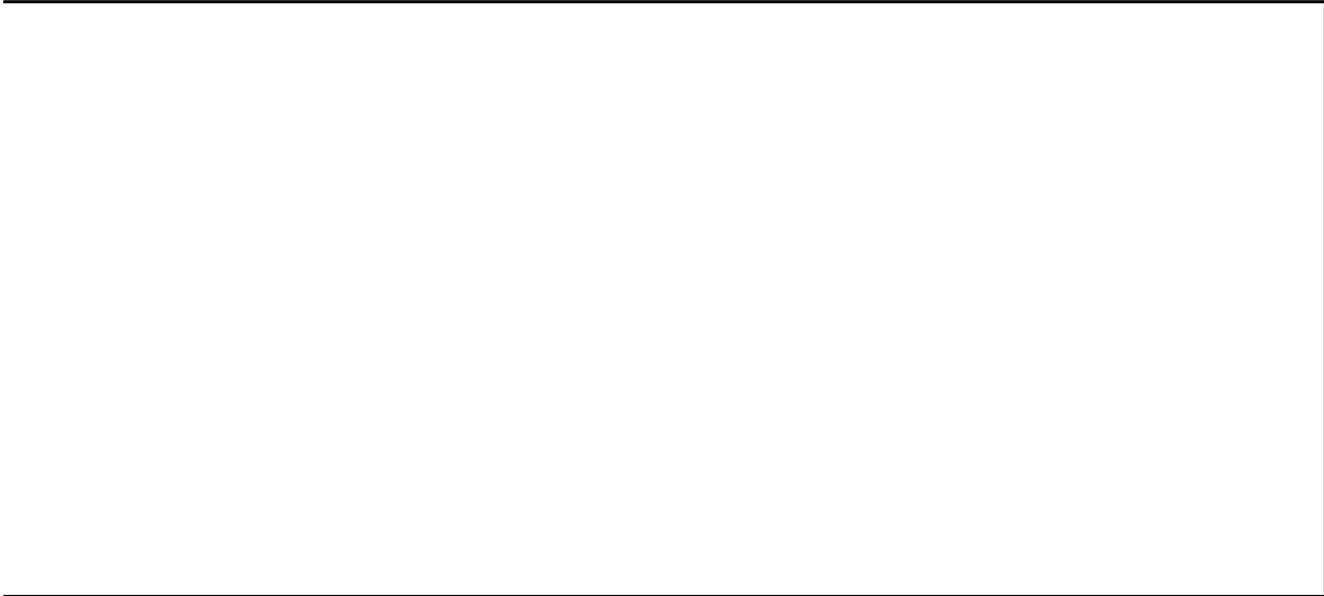
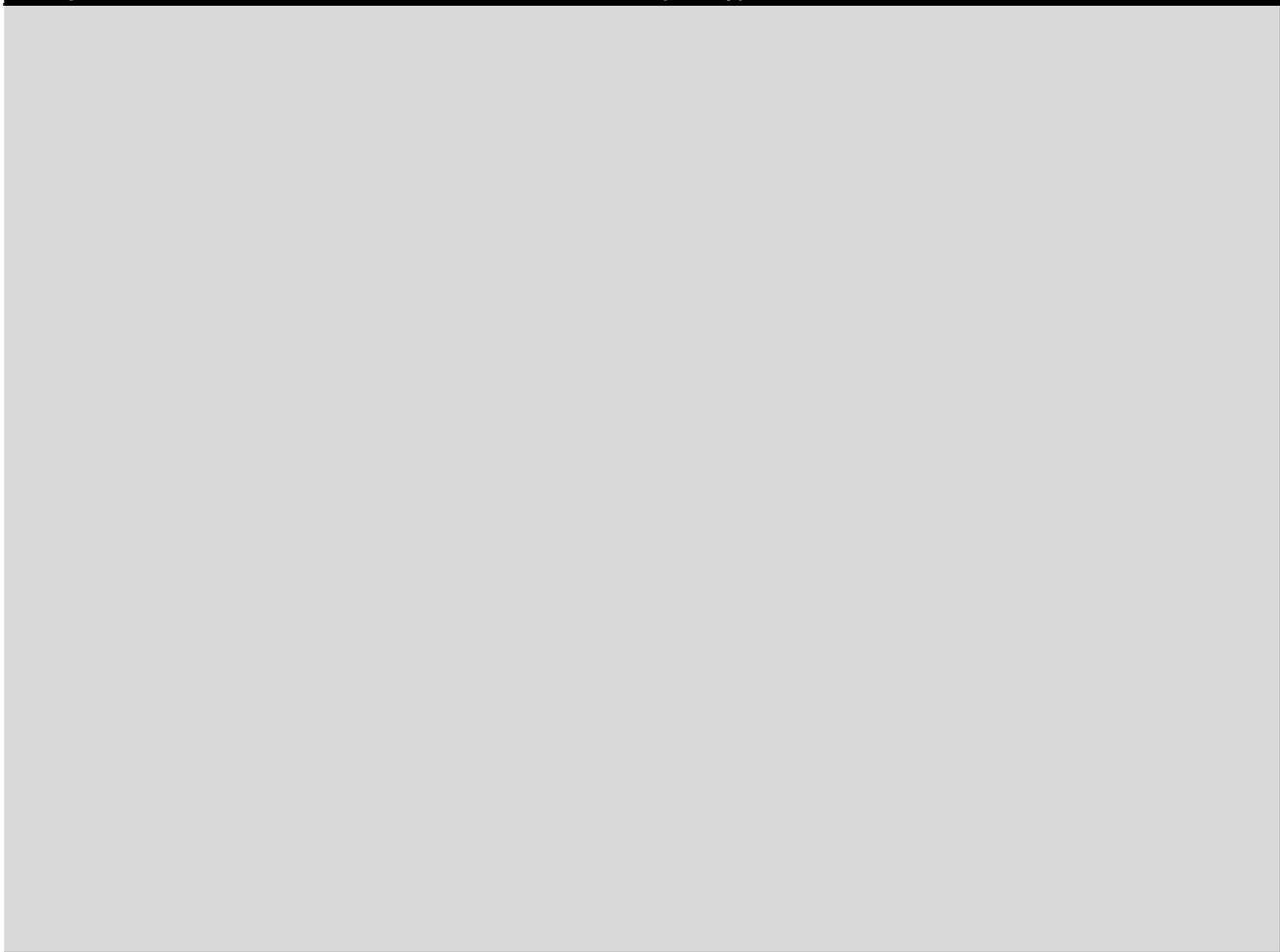
§164.414(b)

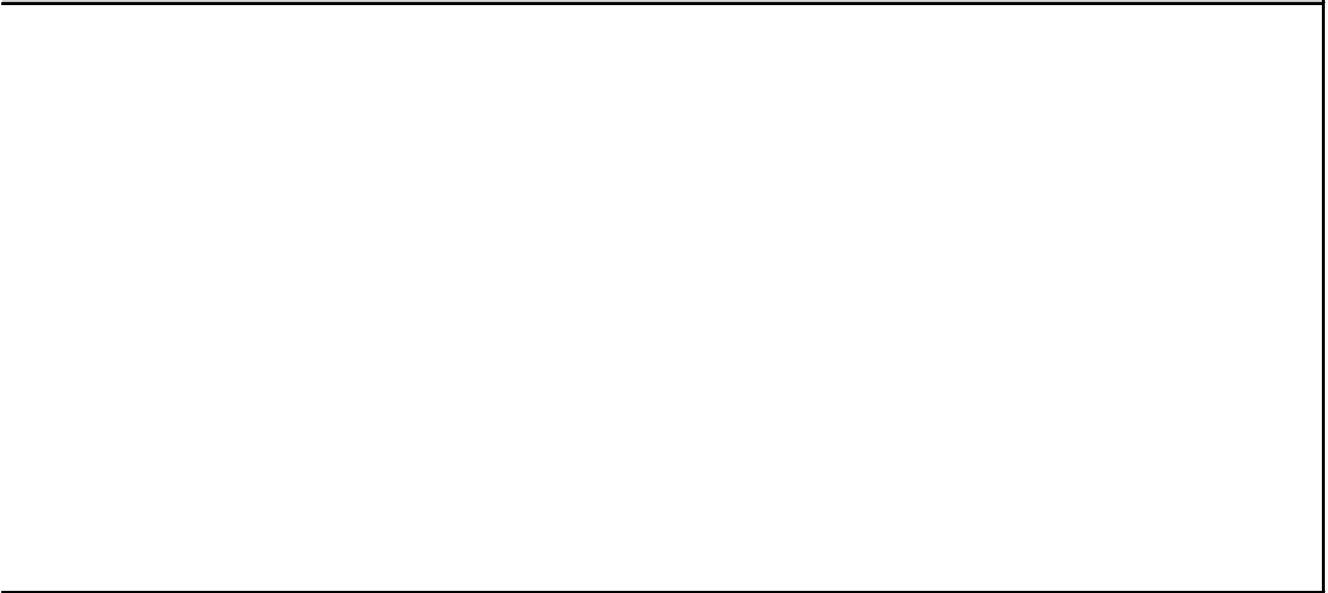
Burden of proof

Required/ Addressable

Evidence (Policy)

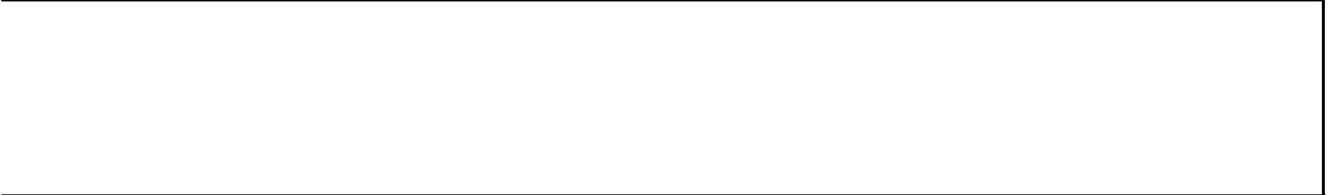
Comments

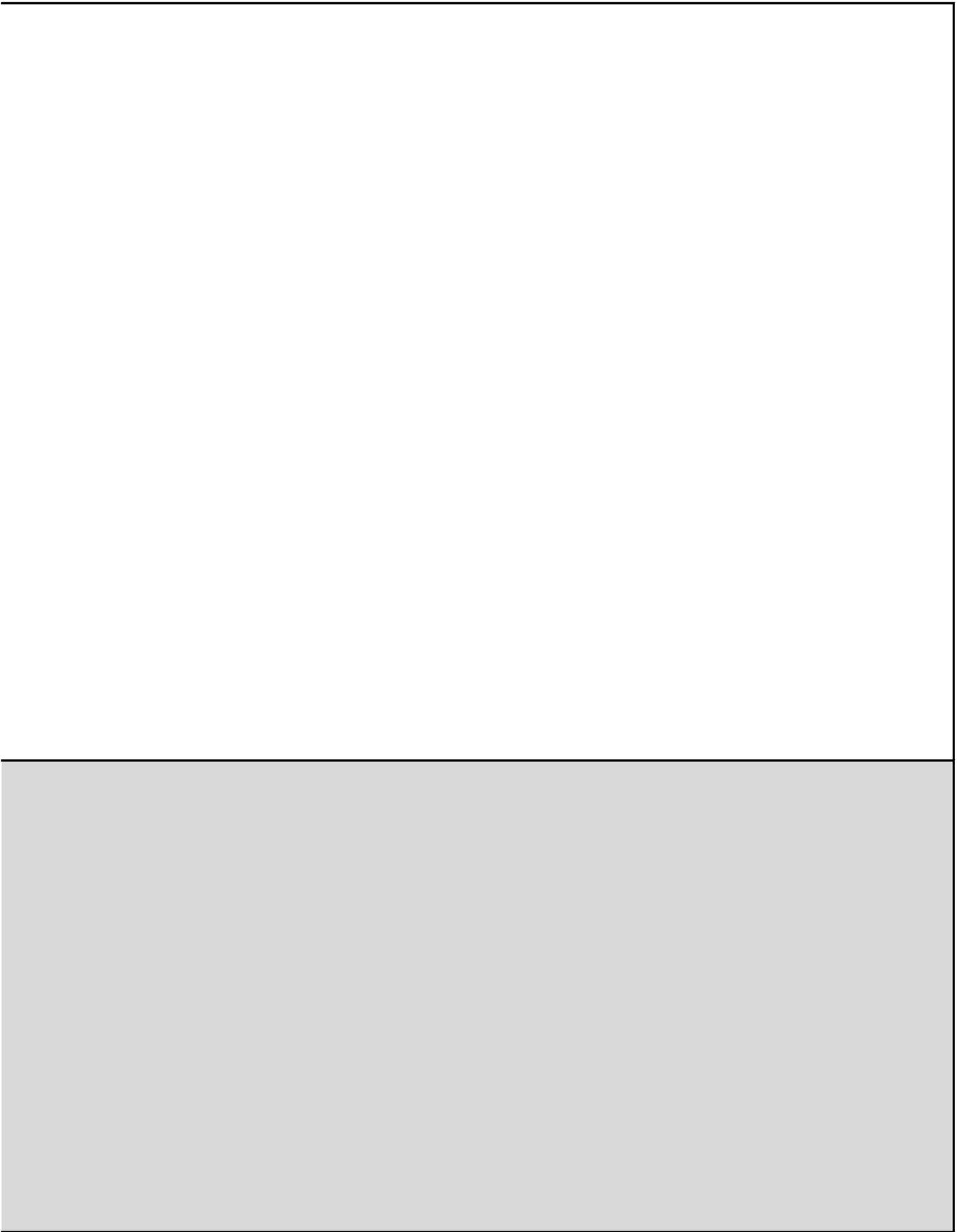








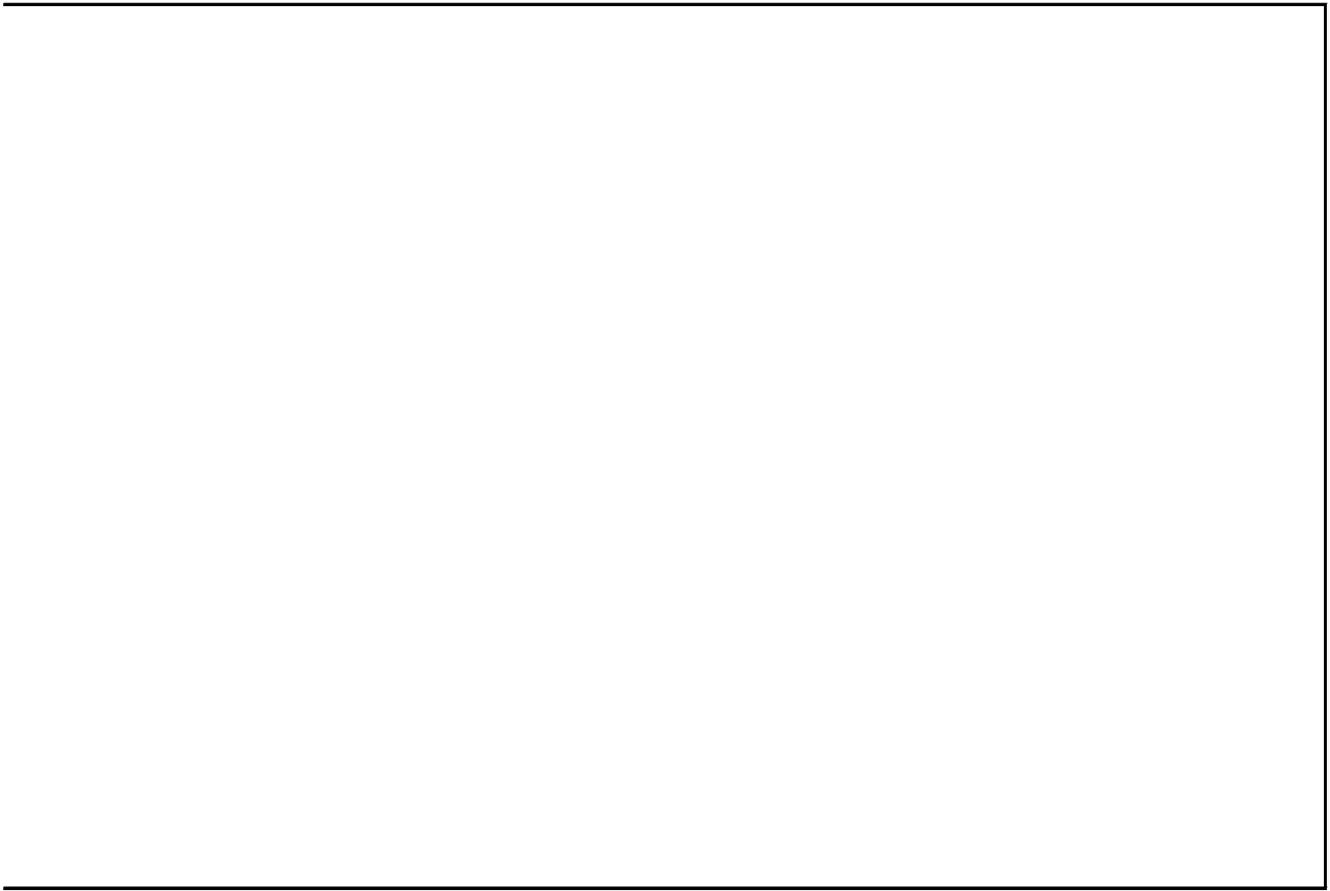


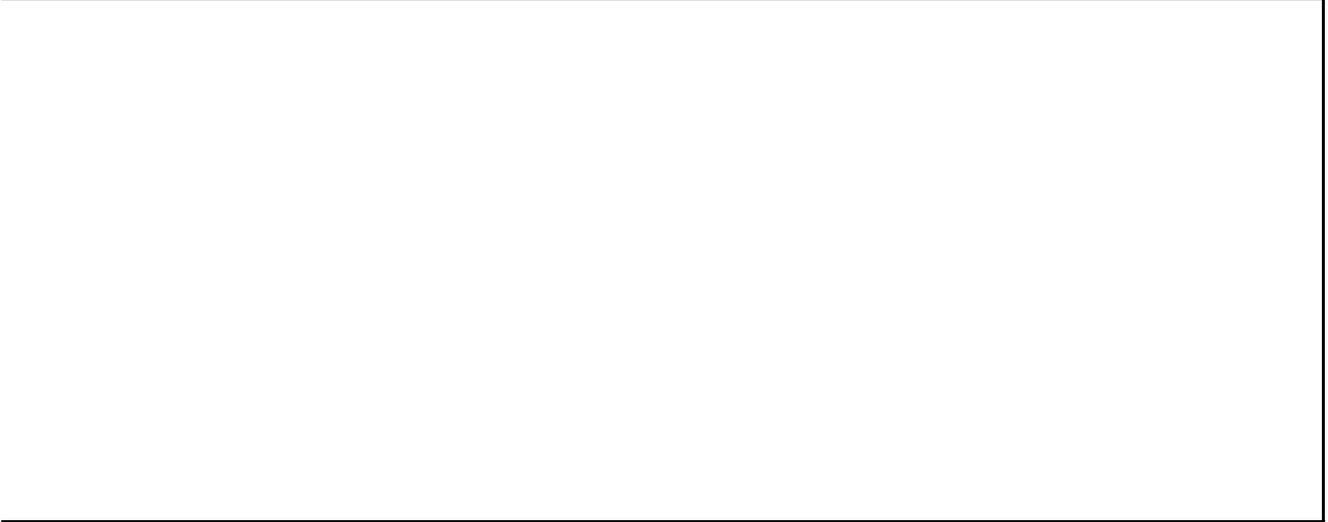


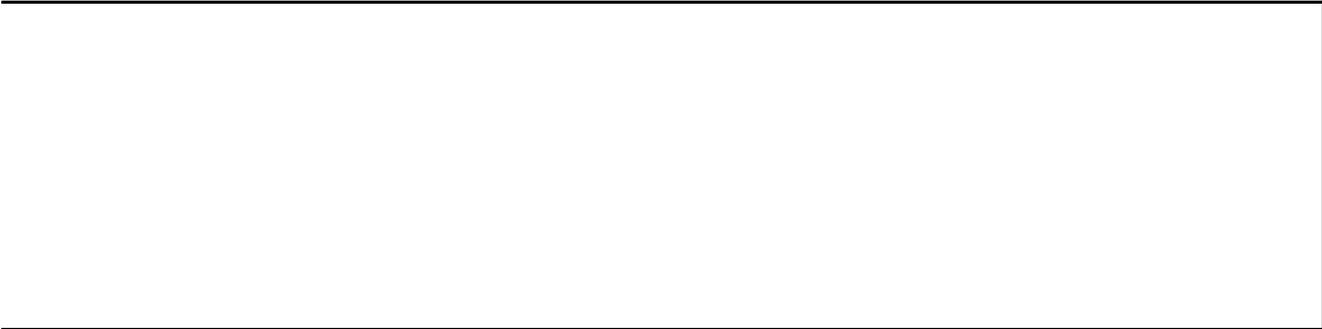
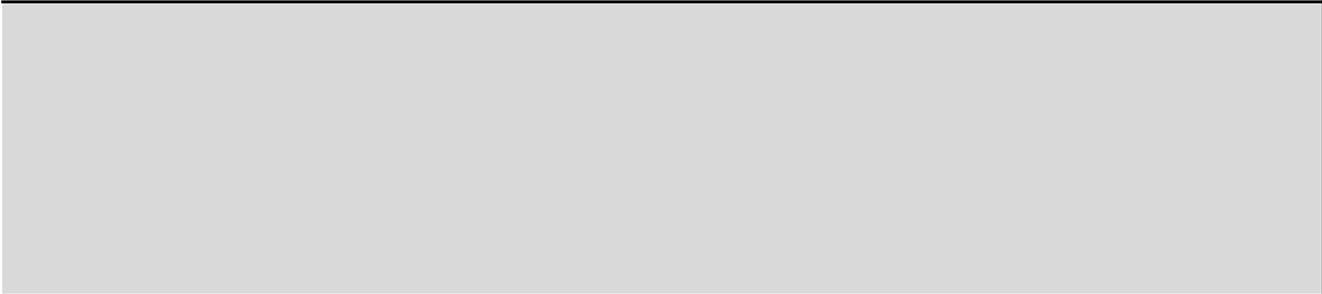
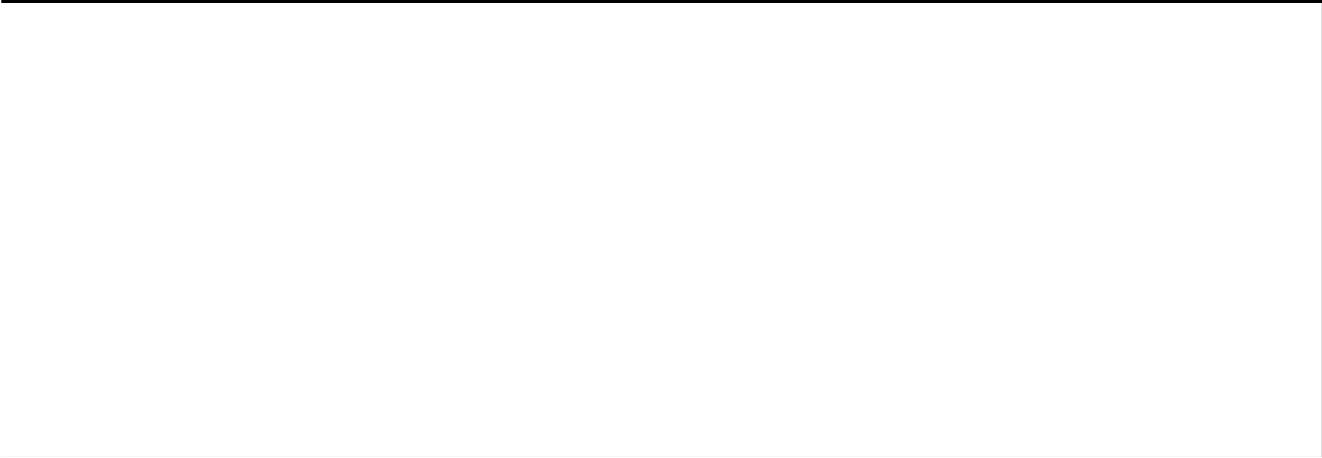
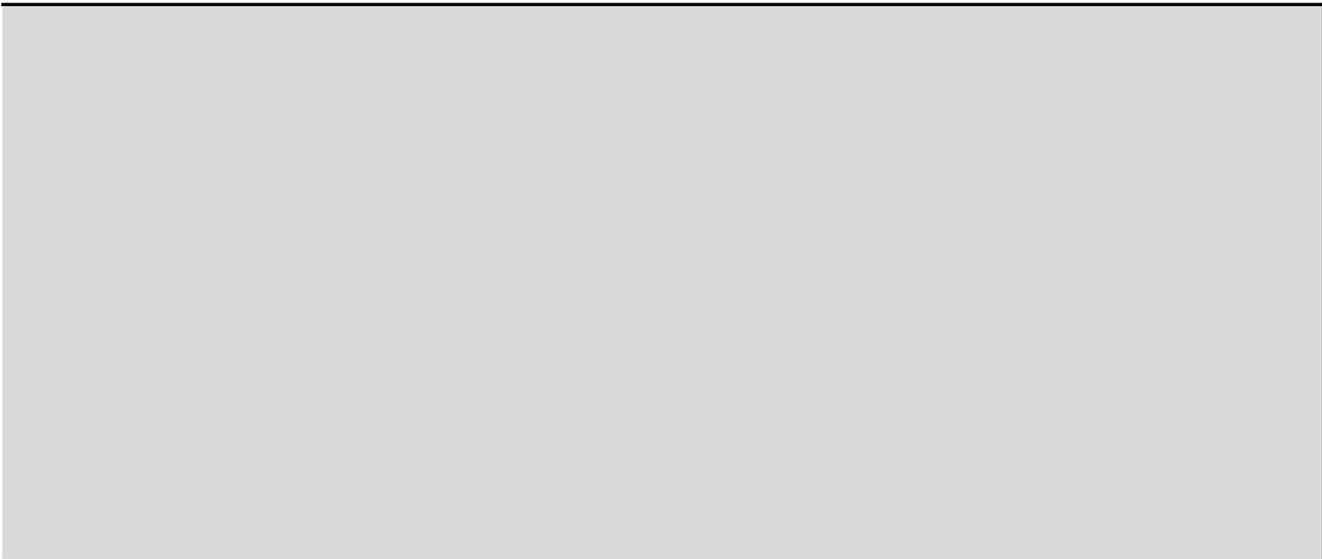




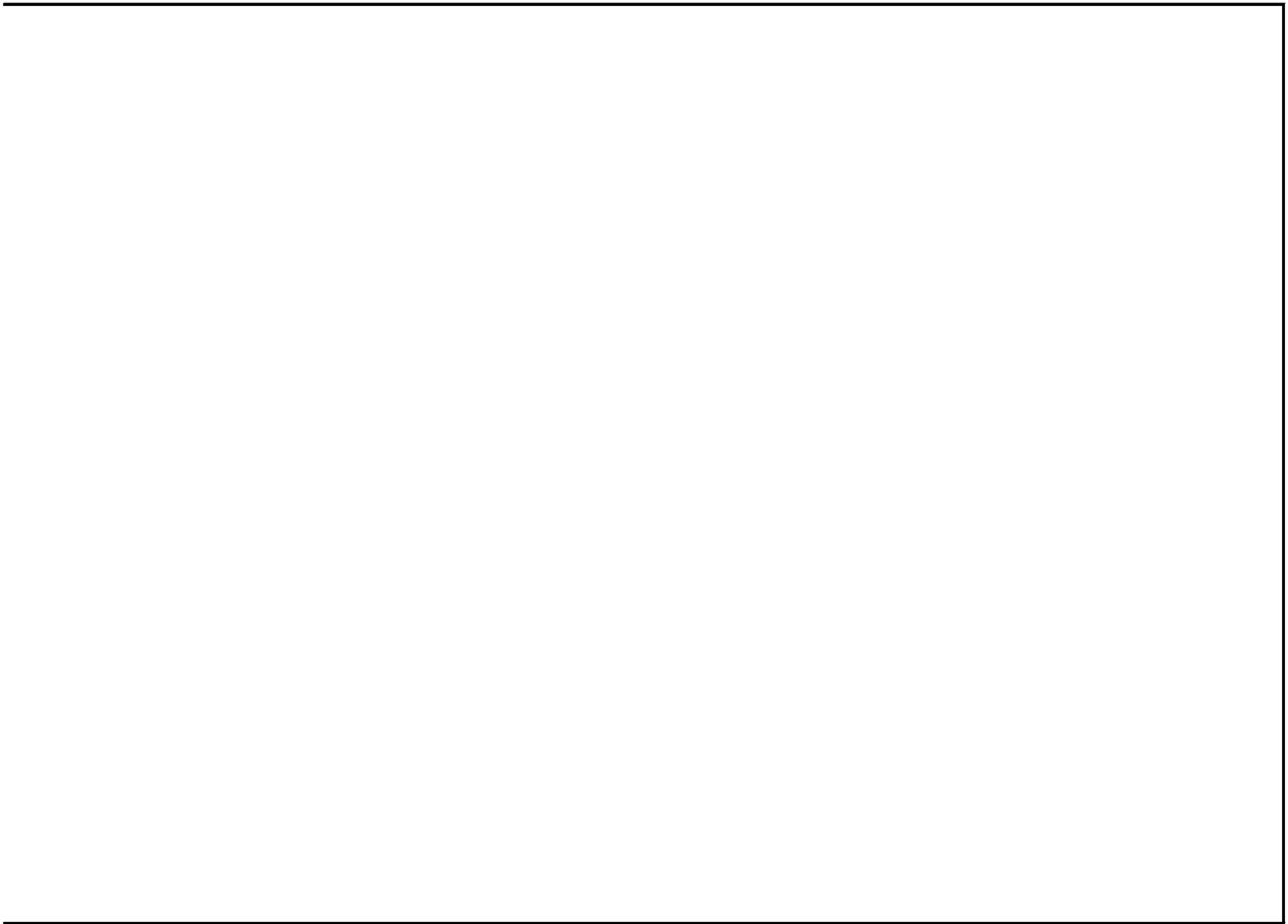


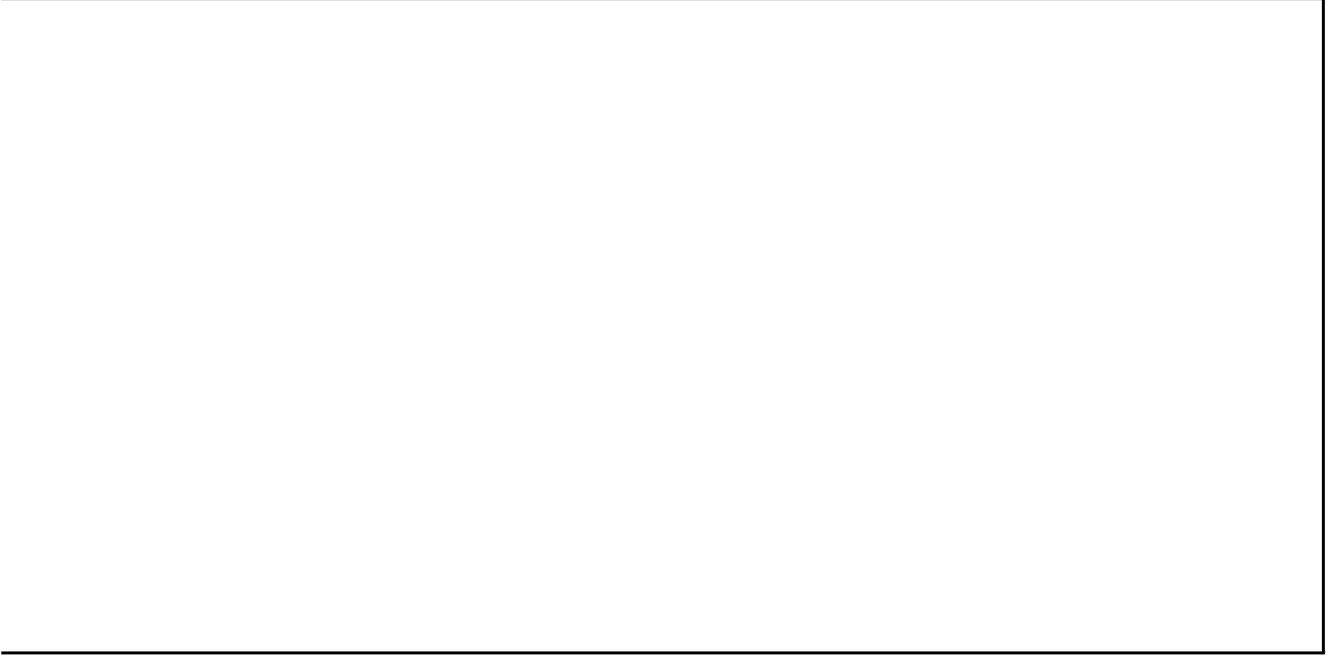






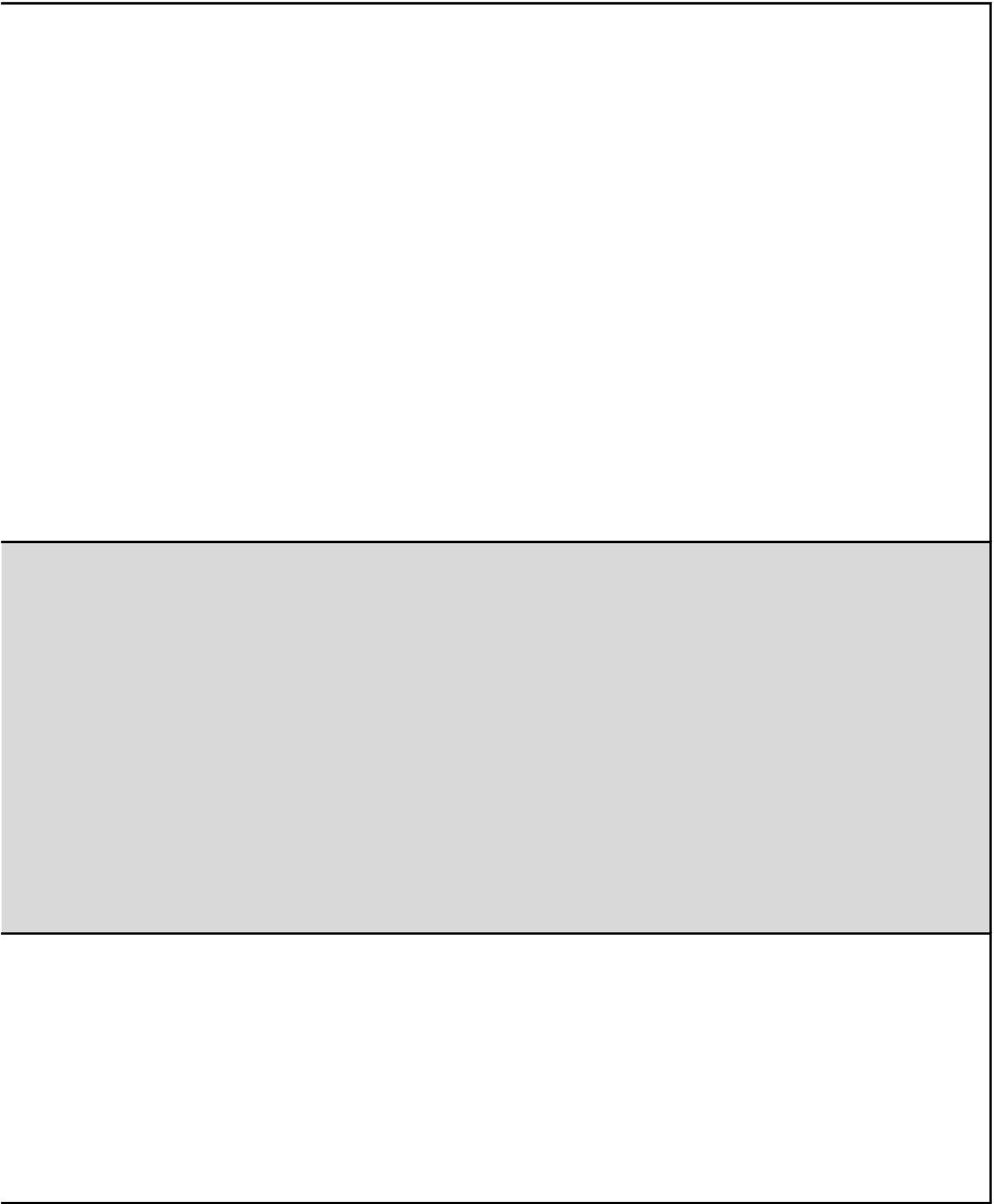








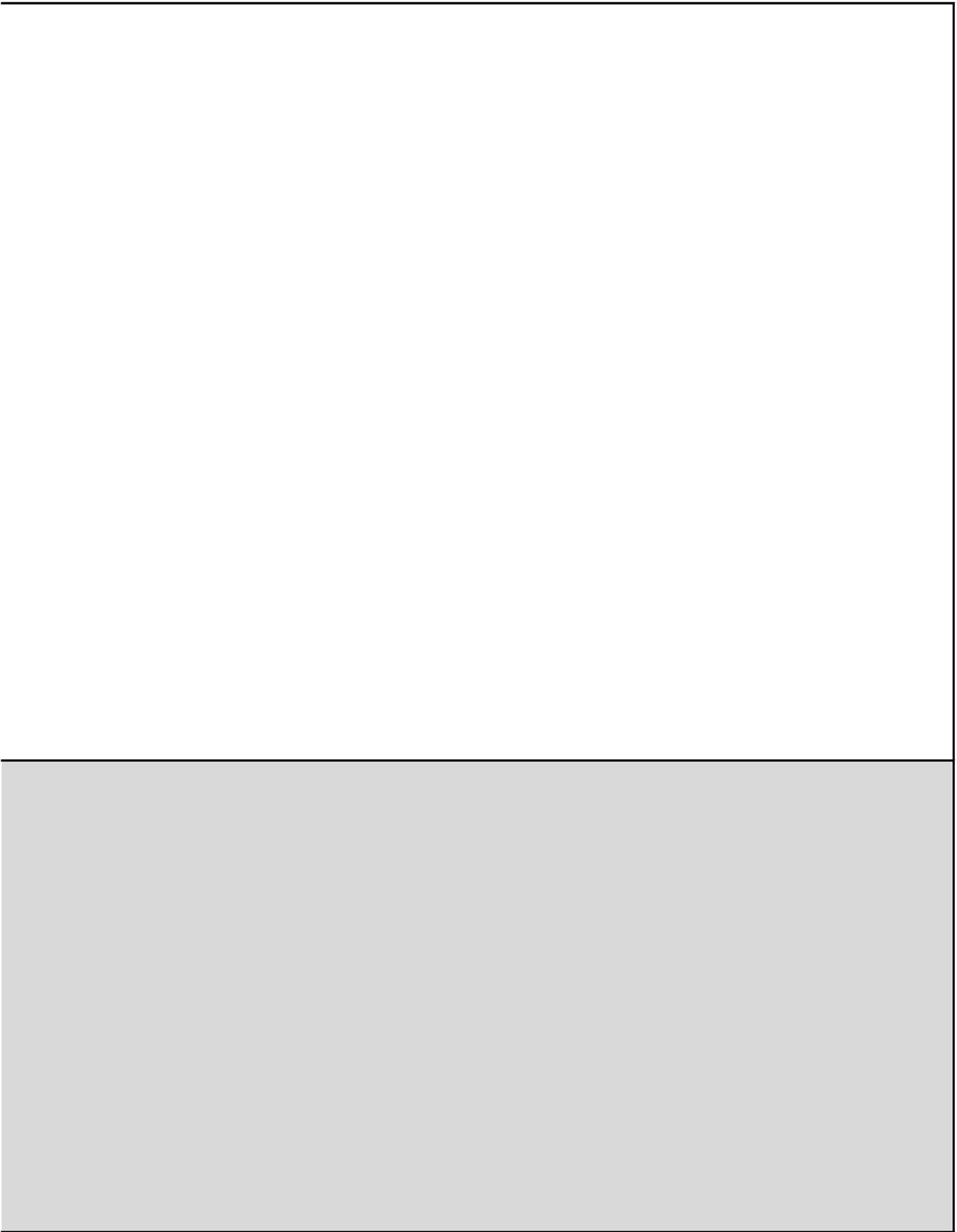


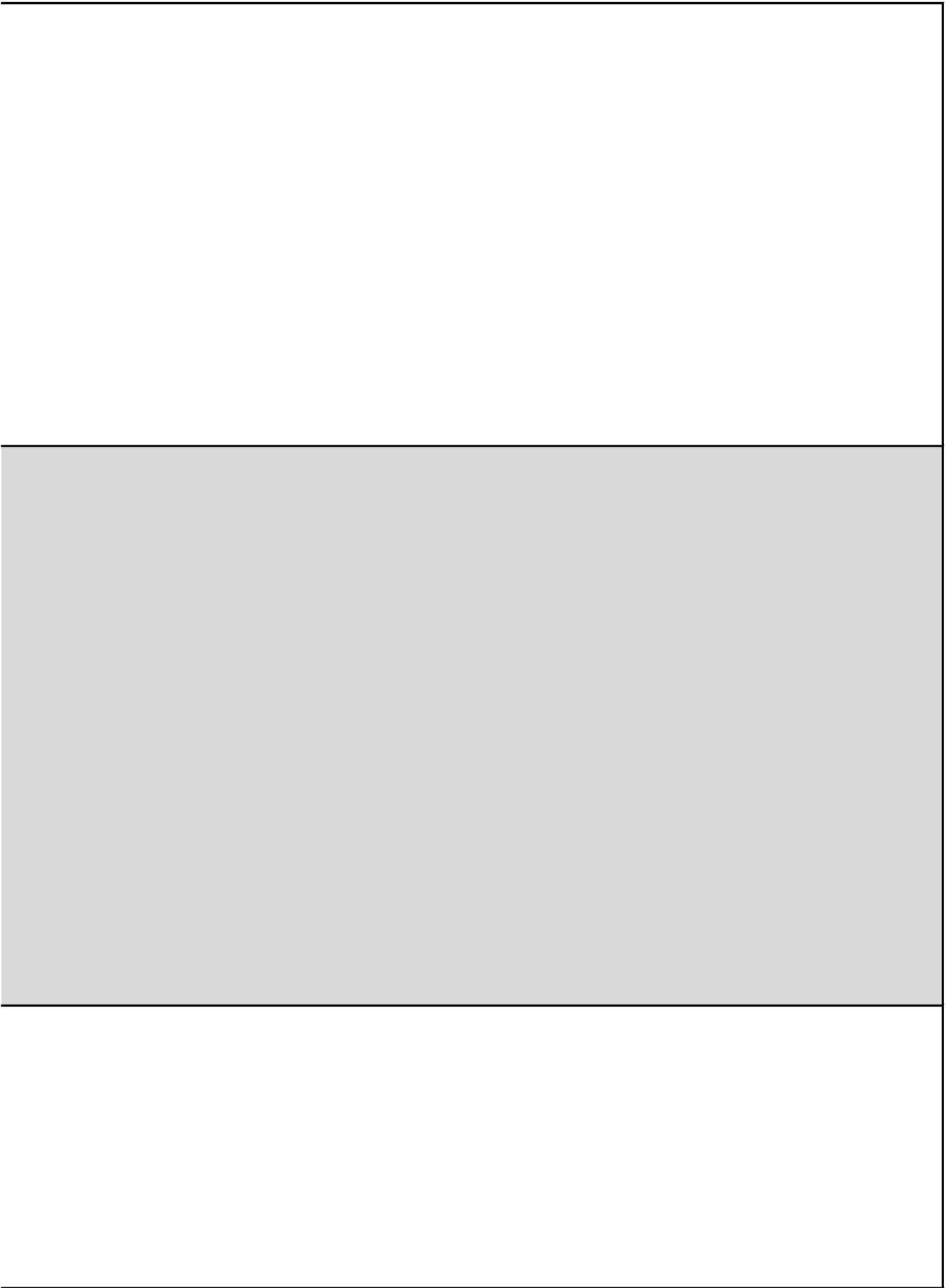




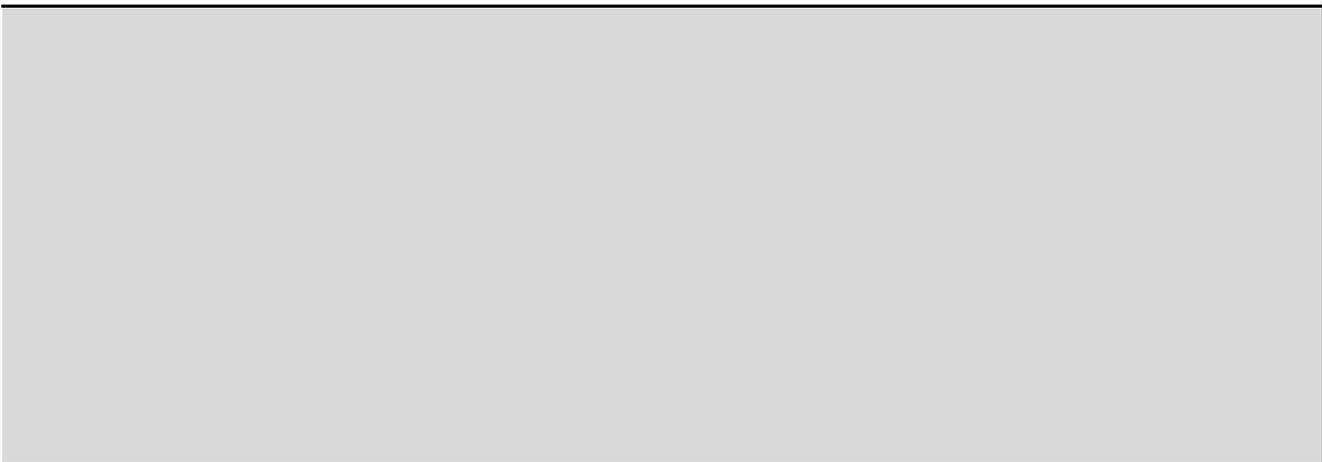


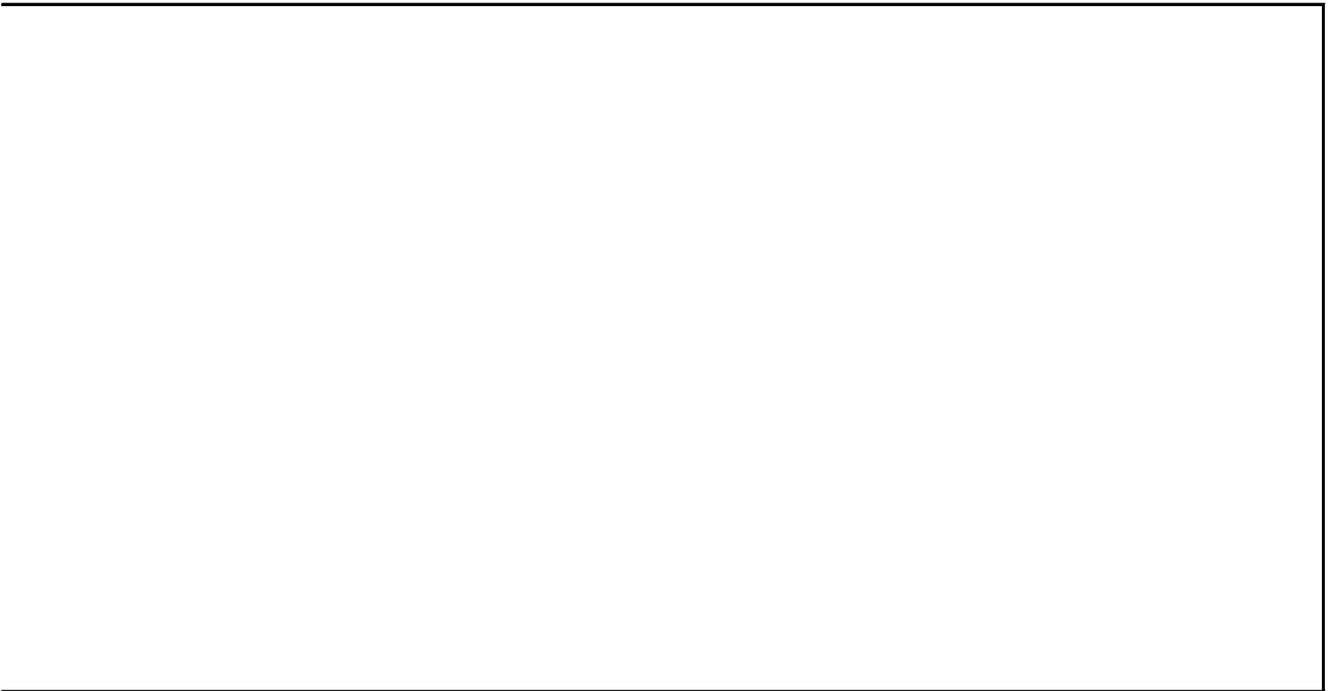


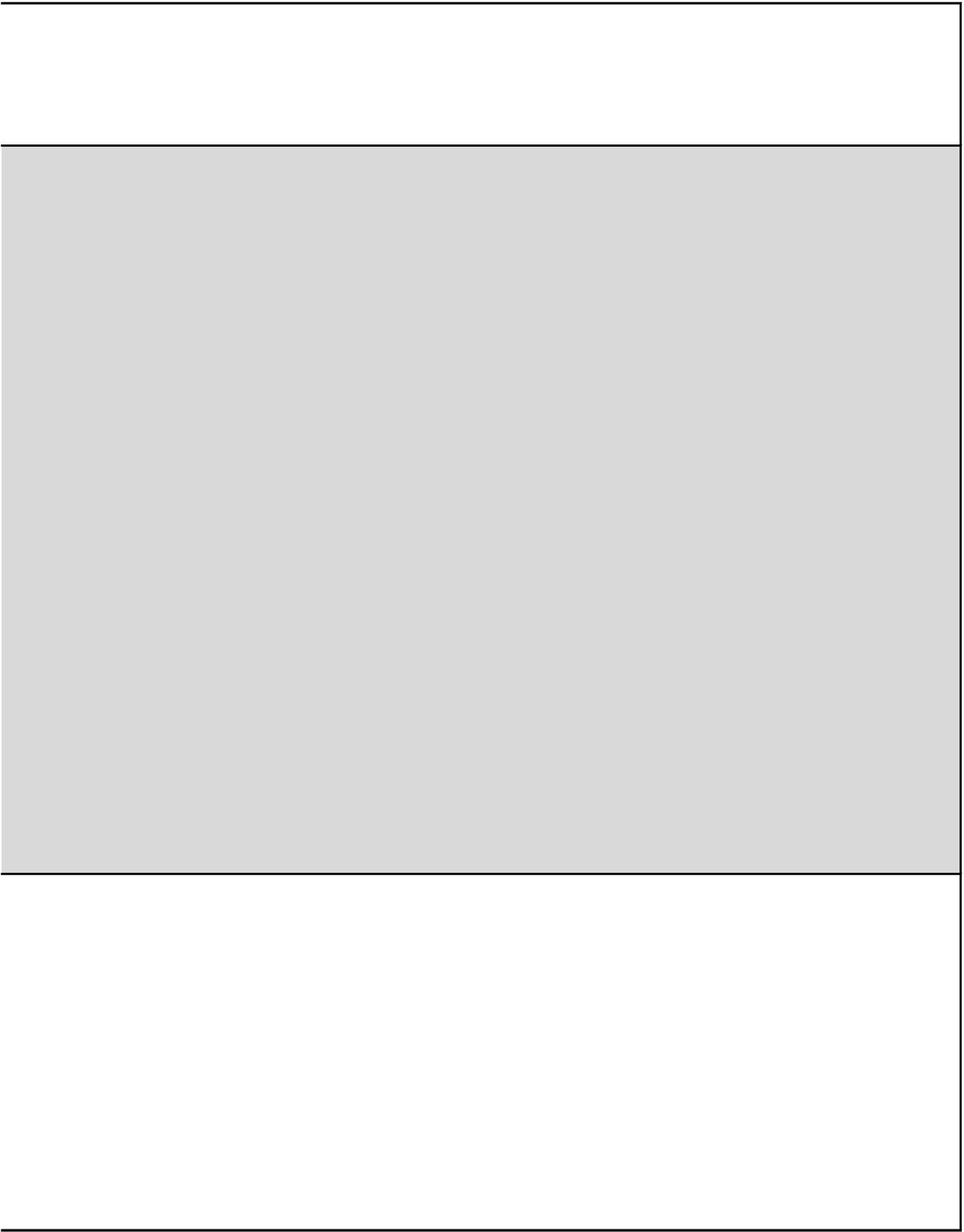


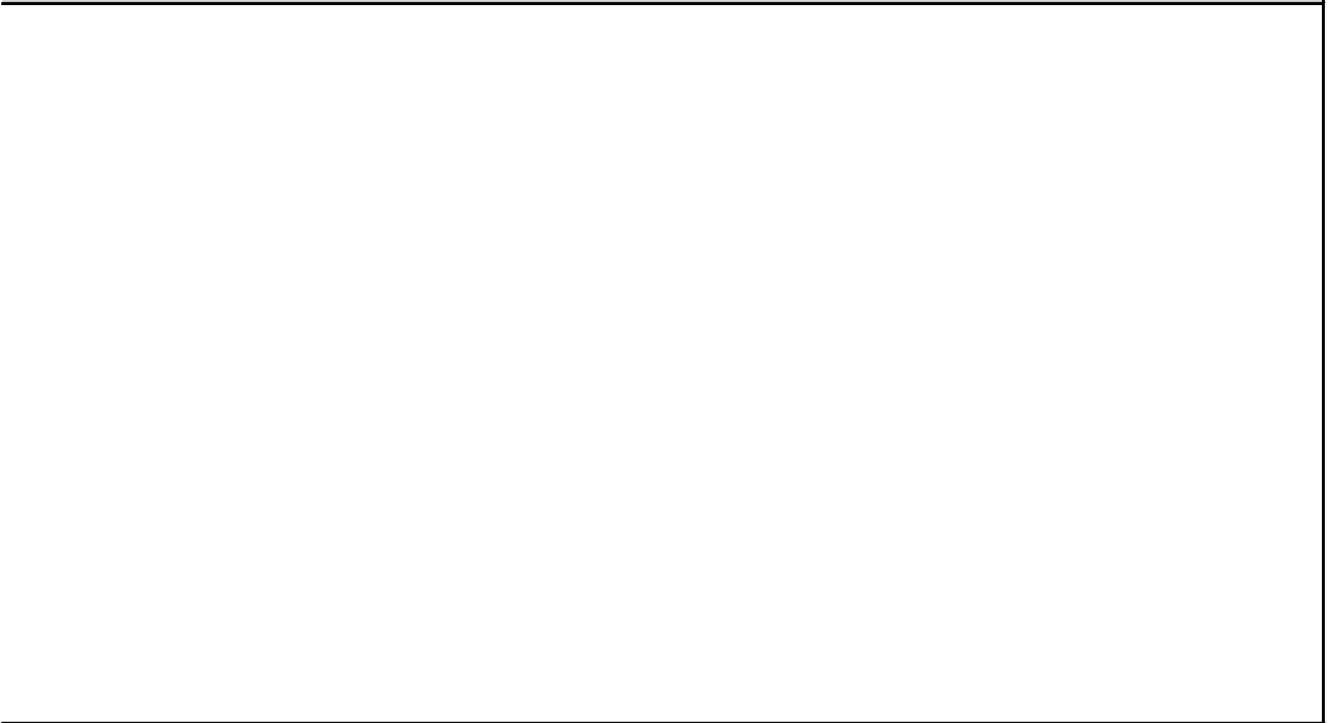


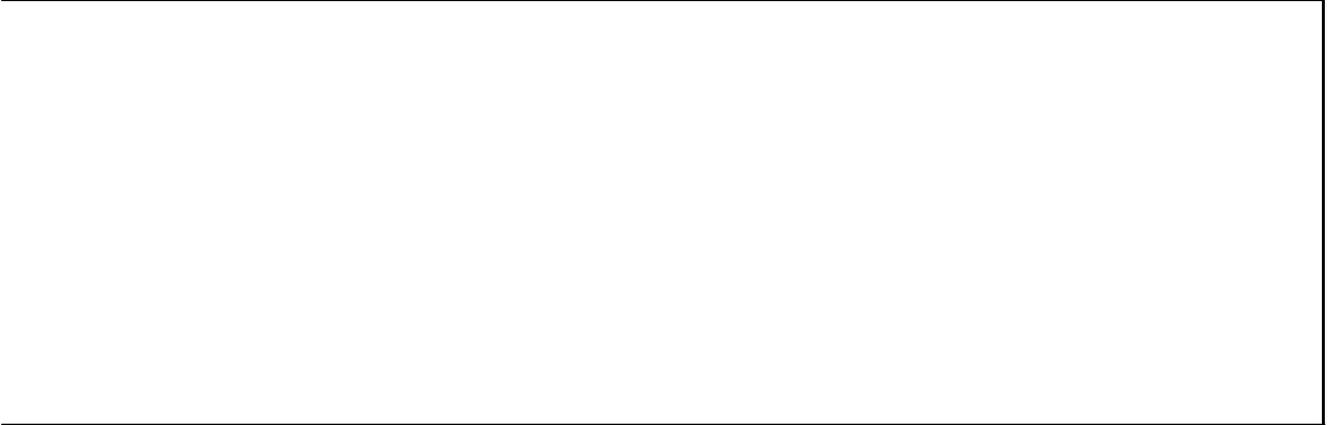




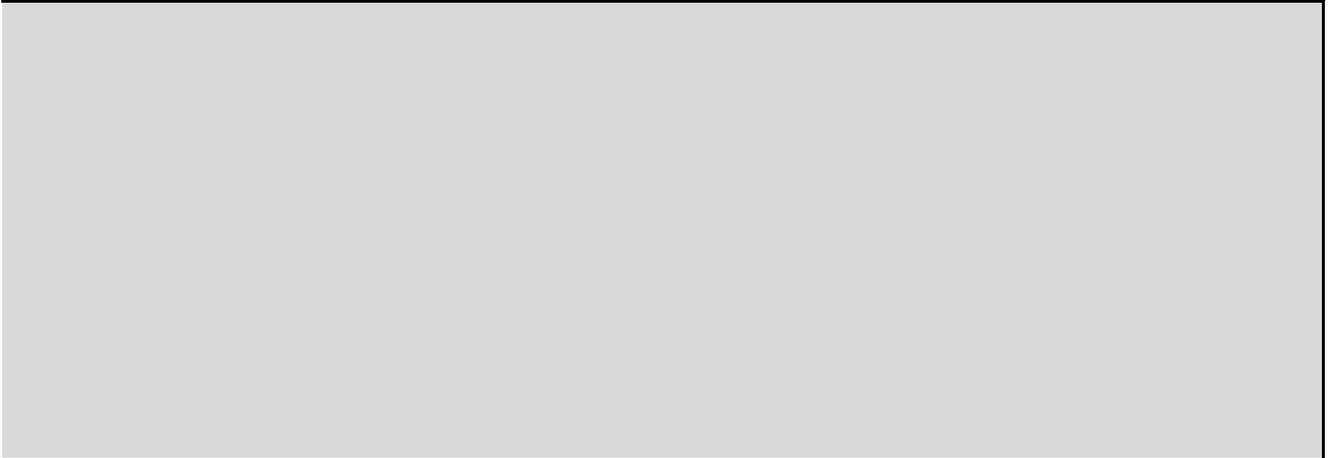
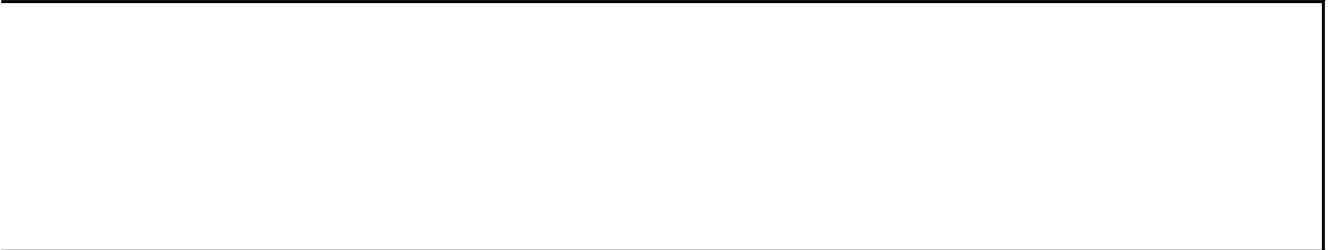


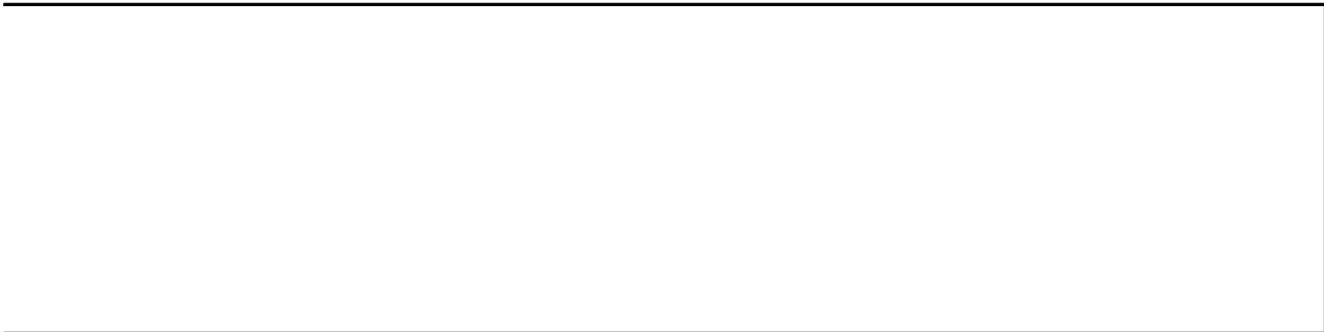












R

R

R

R

R

R

A

A

A

R

R

A

A

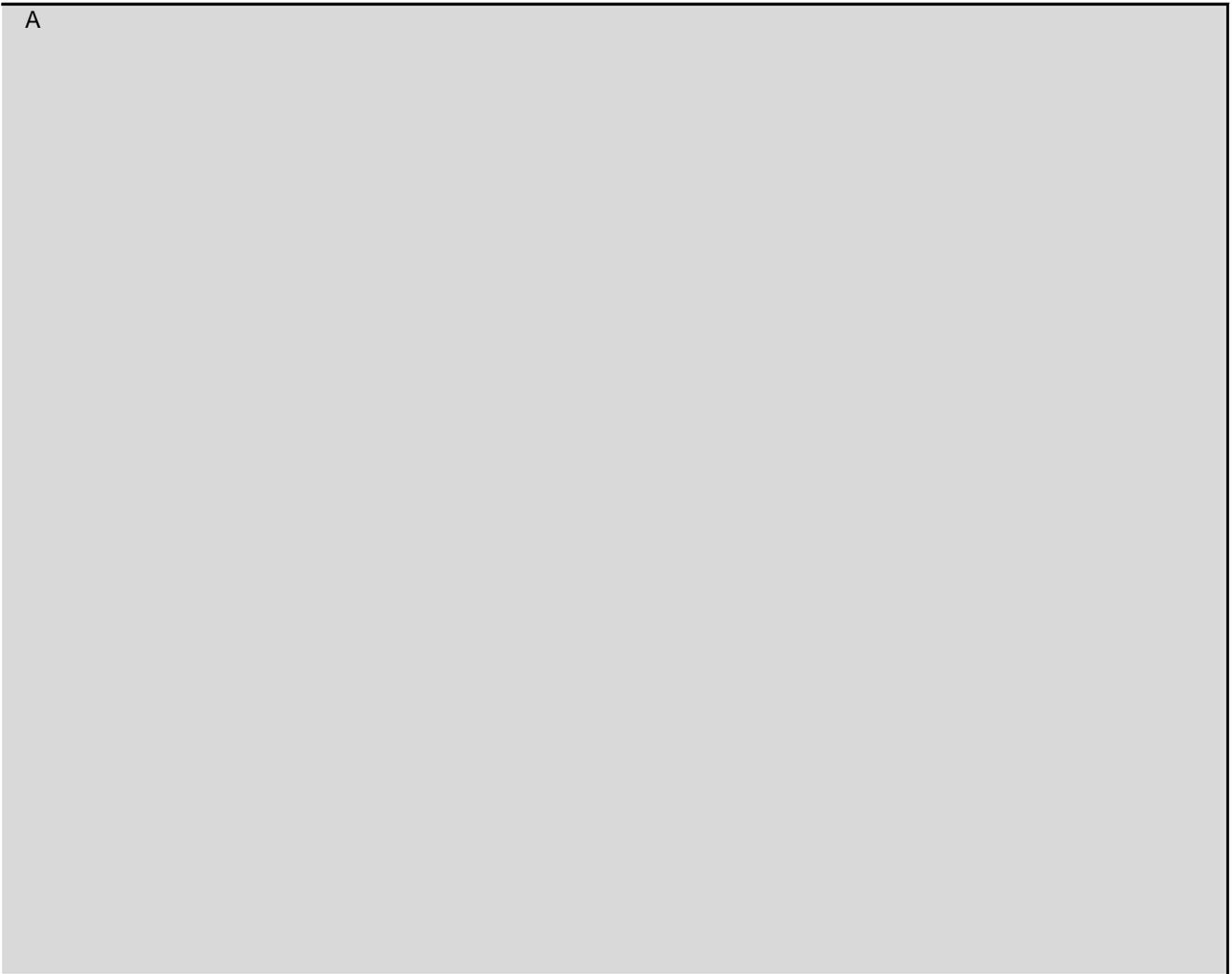
R

A

A

A

A



R



R

R

R

R

R

A

A

R

R

R

R

A

A

A

A

R

R

R

R

R

A

A

R

R

R

A

A

R

R

A

R

R

A

A

R

R

R

R

R

R

R

R

R

R

R

R

R

R

R

R



